

CCNP

Cisco Certified
Network Professional

Course Presentation



CCNP

(Cisco Certified Network Professional)

Certification Mapped Course

Route, Switch and Troubleshoot

Course Presentation

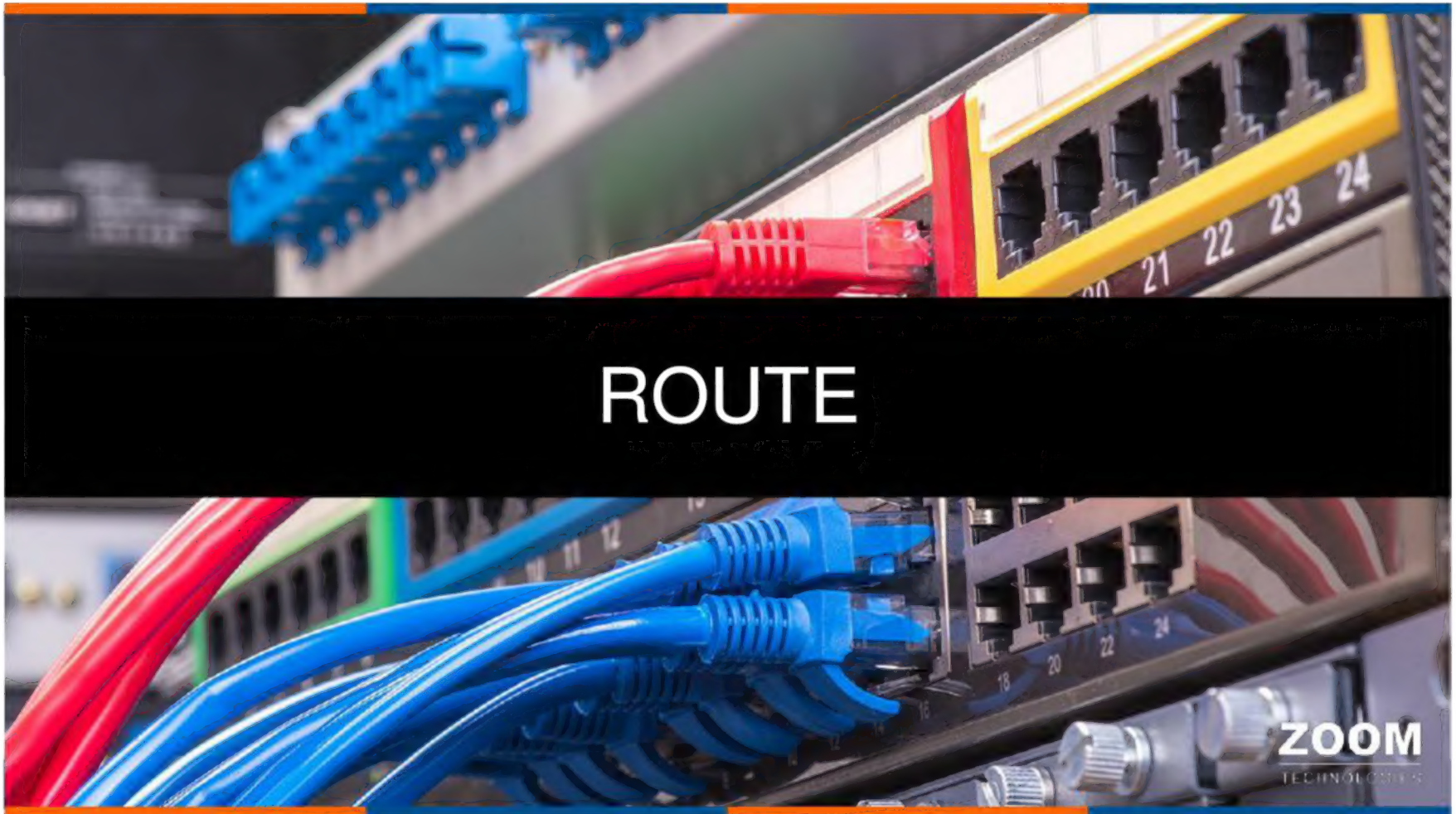


© 2015 Zoom Technologies India Pvt. Ltd.

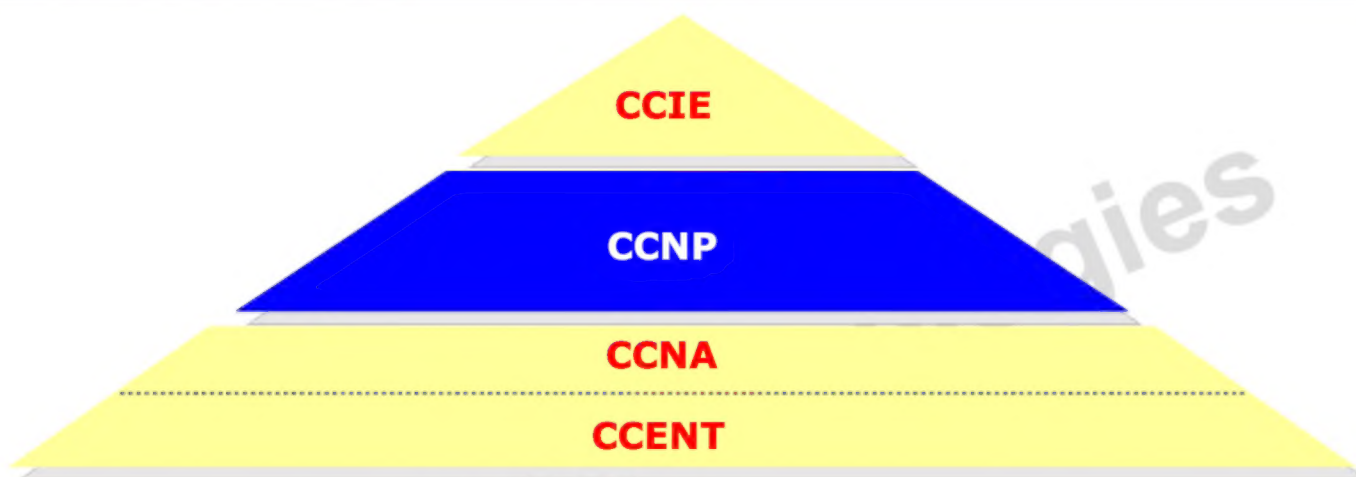
All rights reserved. No part of this book or related material may be reproduced in any form or by any means without prior permission from Zoom Technologies India Pvt. Ltd. All precautions have been take to make this book and related material error-free. However, Zoom Technologies India Pvt. Ltd. is not liable for any errors or omissions. The contents of this book are subject to change without notice.

DISCLAIMER: CISCO, CCNA, CATALYST are registered trademarks of Cisco Inc.



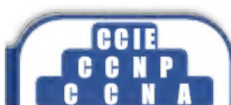


Cisco Certification tracks



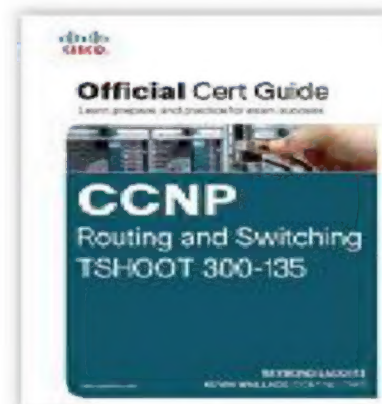
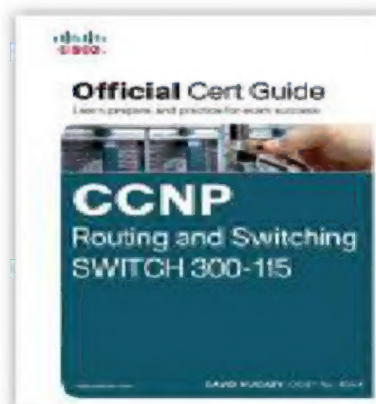
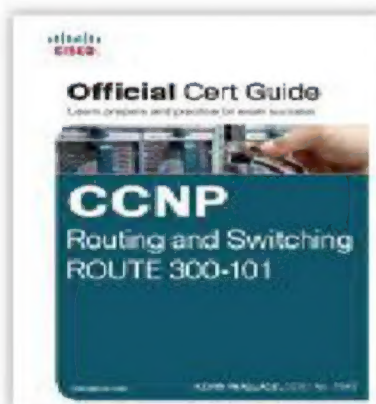
CCNP Routing and Switching Version 2

validates the ability to plan, implement, verify and troubleshoot local and wide-area enterprise networks

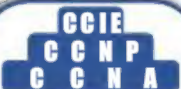


- **ROUTE (300-101)**
 - Implementing Cisco IP Routing
- **SWITCH (300-115)**
 - Implementing Cisco IP Switched Networks
- **TSHOOT (300-135)**
 - Troubleshooting and Maintaining Cisco IP Networks

Zoom Technologies



Zoom



- **Pre-requisites:**

(valid cisco CCNA Routing and Switching Certification)

- **Exam Details:**

Register	: Pearson VUE
Duration	: 120 minutes
Number of question	: 45-65 questions (R&S) : 15-25 Question (t-shoot)
Available Languages	: English
Type of Question	: Multiple choice ,Testlet ,Drag and Drop , Simulated Lab ,Simlets
Passing Score	: 790/1000



IP Addressing

- **Two Versions of Addressing Scheme**

- IP version 4 – 32 bit addressing
- IP version 6 – 128 bit addressing



- Total IPv4 Addressing Scheme is divided into 5 Classes

- CLASS A
 - CLASS B
 - CLASS C
 - CLASS D
 - CLASS E
- LAN and WAN – Unicast**
- Multicasting**
- Research and Development**

Class	Range	Octet Format	Subnet Mask	Cisco / Notation
Class A	0.0.0.0 to 127.255.255.255	N.H.H.H	255.0.0.0	/8
Class B	128.0.0.0 to 191.255.255.255	N.N.H.H	255.255.0.0	/16
Class C	192.0.0.0 to 223.255.255.255	N.N.N.H	255.255.255.0	/24
Class D	224.0.0.0 to 239.255.255.255	N/A	N/A	N/A
Class E	240.0.0.0 to 255.255.255.255	N/A	N/A	N/A

What is a Router ?

- **A Router** is a internetworking Device.
- It routes the packet from one logical network to another logical network
- It has two main functions.
 - Determination of best path towards destination.
 - Switching packet from inbound interface to outbound interface.

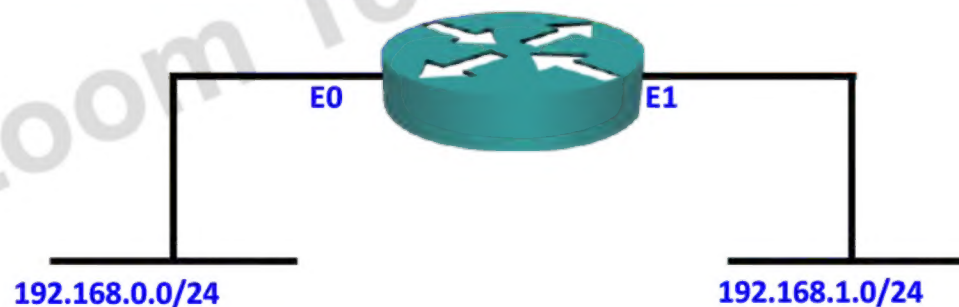


Routing

- Forwarding the packet from one network to other network.
- Routing is enabled by default

To enable or disable IP Routing

Router(config)# [no] ip routing



Types of Routing

- Static Routing
- Dynamic Routing

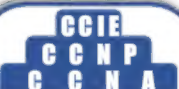
Zoom Technologies

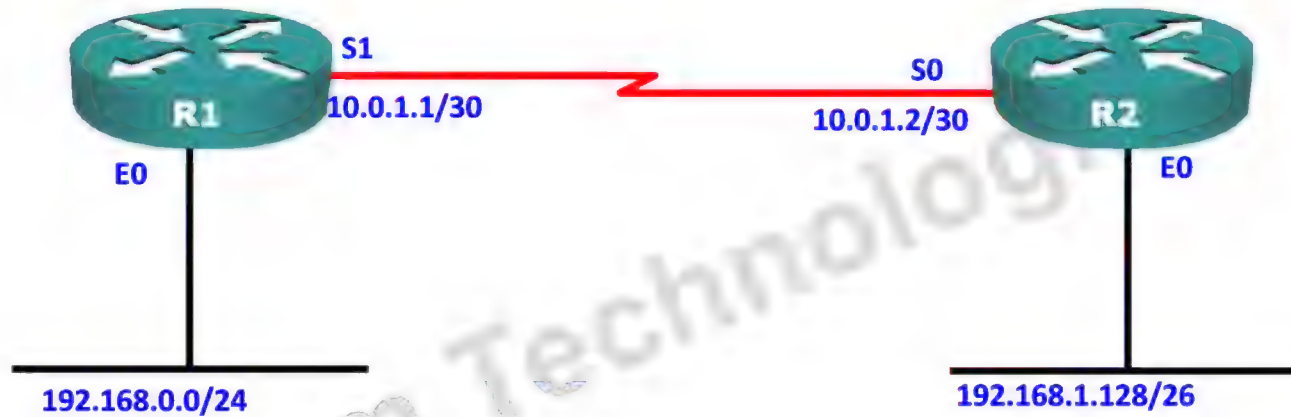


Static Routing

- Manually configured by Administrator
- Administrative distance is 1
- Destination network should be known
- Routing based on next hop IP address or exit interface
- Secure and fast

Zoom Technologies



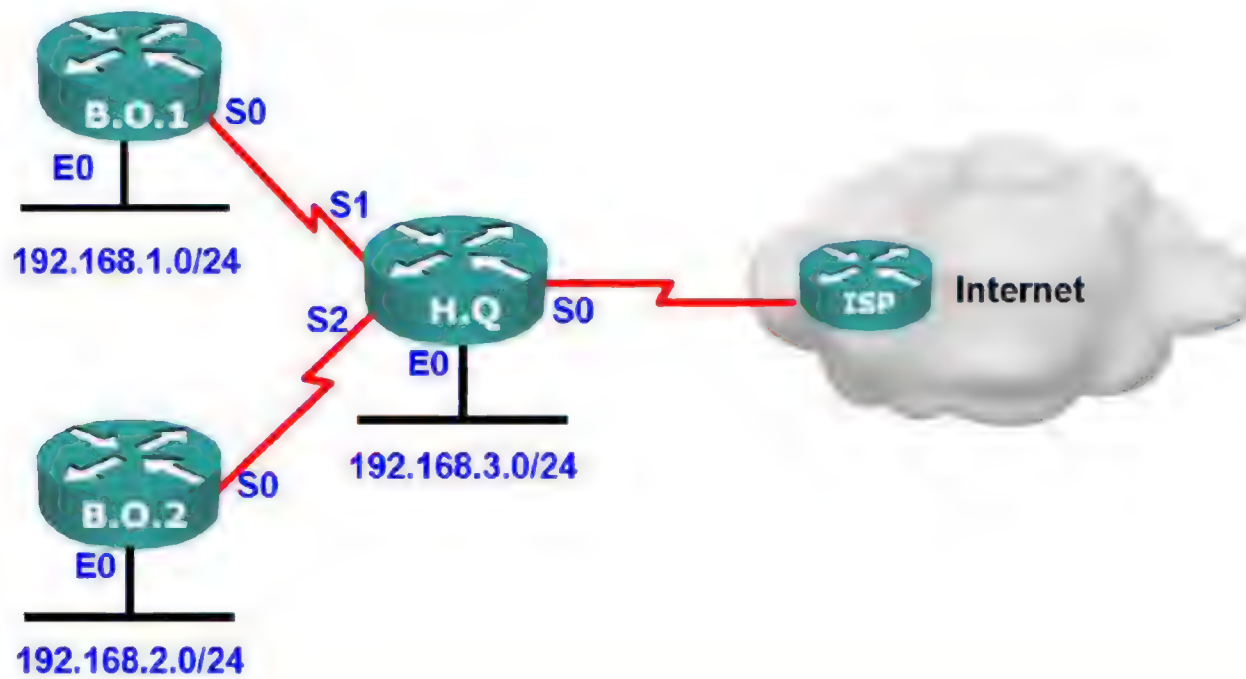


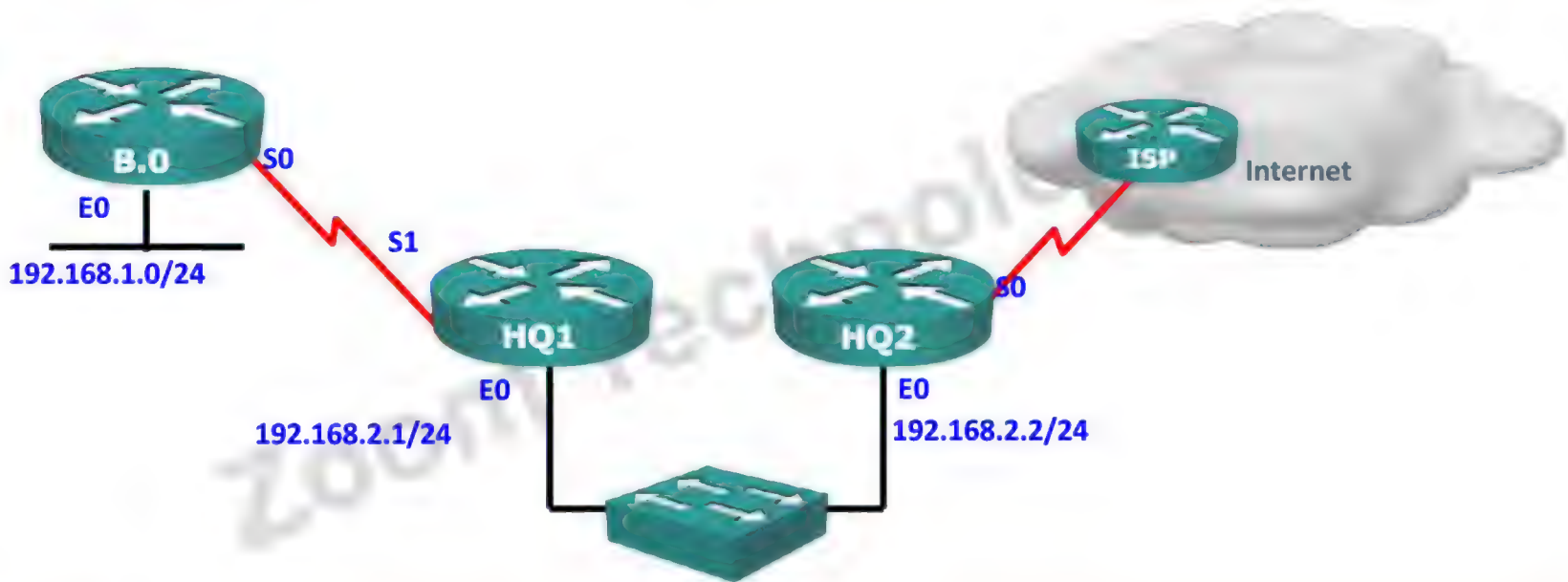
- Static default route will be used for unknown destinations
- It may be used for accessing the Internet.
- It can be also used on a Stub router.
- It is least preferred route in the routing table.
- The router uses this route only when it cannot find a more suitable match in the routing table.

Default route configuration.



Static and Default routing Example

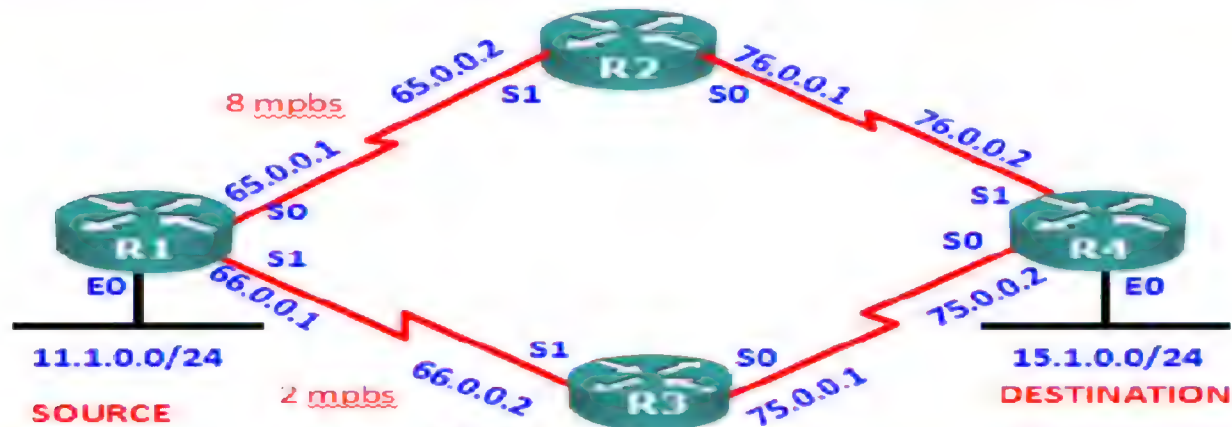




Floating Static Route

- Floating static routes are static routes that are used to provide a backup path to a primary static route, in the event of a link failure.
- The floating static route is only used when the primary route is not available.
- To accomplish this, the floating static route is configured with a higher administrative distance than the primary static route.

Floating Static Route



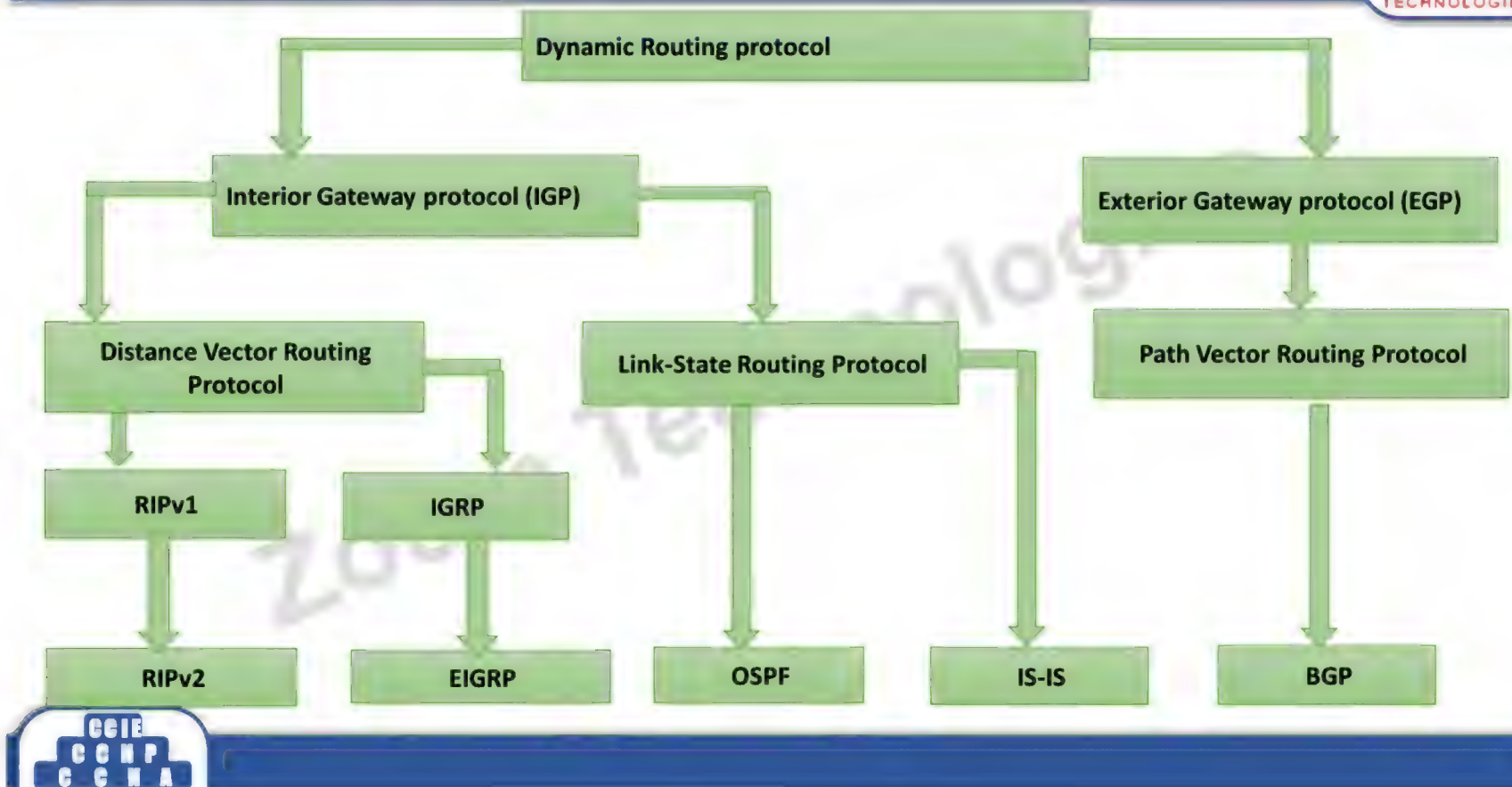
Floating Static Route Configuration

```
R1(config)# ip route 15.1.0.0 255.255.255.0 65.0.0.2
```

```
R1(config)# ip route 15.1.0.0 255.255.255.0 66.0.0.2 7
```

Dynamic Routing Protocol

- Dynamic routing protocols, exchange routing information with the neighbors and build the routing table automatically
- Administrator need to advertise only the directly connected networks
- Any changes in the network topology are automatically updated



- Distance Vector Routing Protocol (RIP, IGRP)
 - Link State Routing Protocol (OSPF, IS-IS)
 - Advanced Distance Vector Routing Protocol (EIGRP)
 - Path Vector Protocol (BGP)
- Zoom Technologies

Summarization



- Combining the contiguous address into one and advertising to neighbor Router
 - Advantages
 - Minimizing the routing table entries
 - Less use of resources like memory, processor, bandwidth
 - Less number of updates
- There are two type of Summarization
 - Auto summary
 - Manual summary

Zoom Technologies



Auto Summary

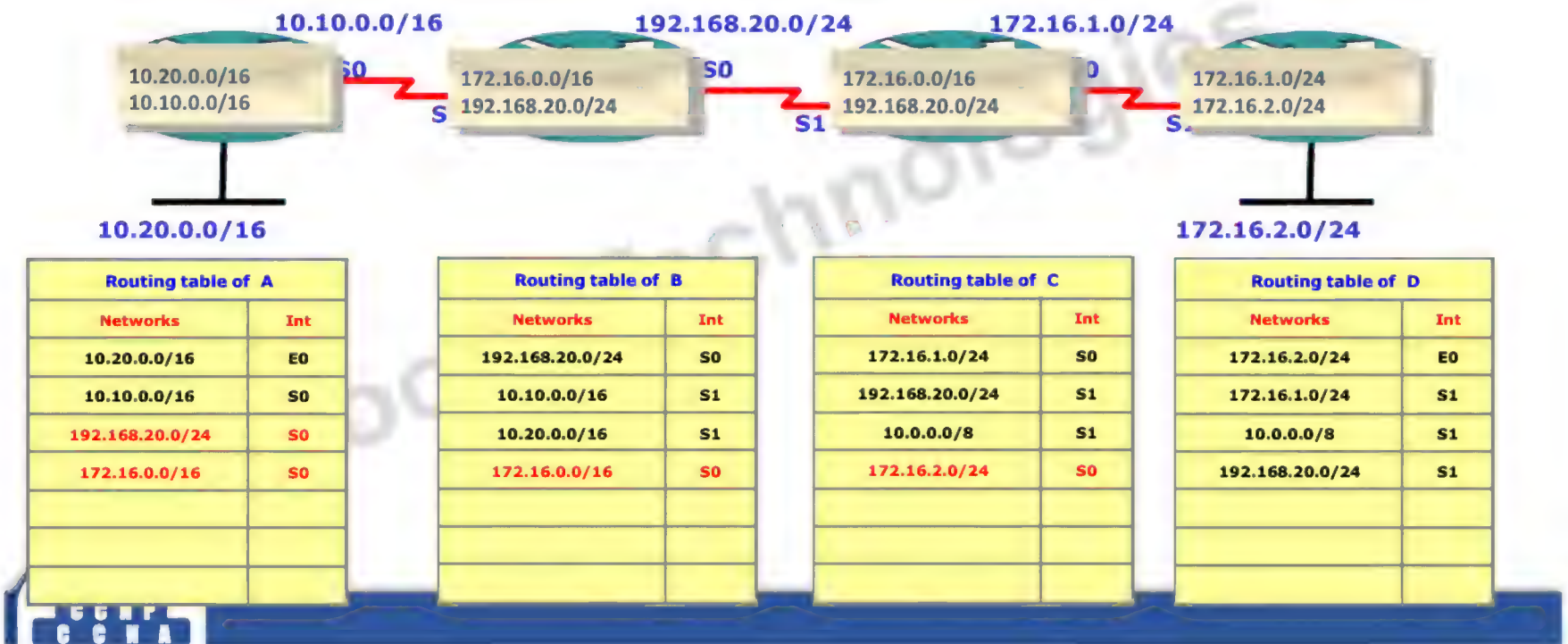


- Subnet at major network boundary will be summarized into class full updates
- A Class full routing protocol does auto summary by default and it cannot be turned off
- Routing protocols like RIPv2, EIGRP, BGPv4 support auto summary
- Link state routing protocol i.e. OSPF and ISIS do not support auto summary

Zoom Technologies



Auto Summary

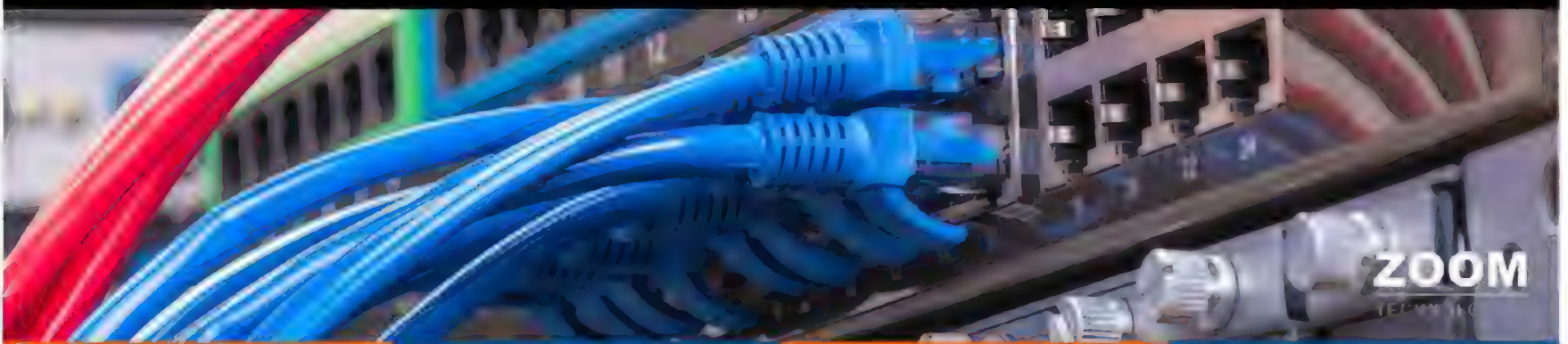


Manual summary

- Administrator manually configures Summarization
- Summary address contains networks in 2n subnets (FLSM)
- It is supported by all classless routing protocols



Enhanced Interior Gateway Routing Protocol



EIGRP Features

- Open Standard
- Advanced distance-vector routing protocol
- Diffusing update algorithm (DUAL)
- Administrative distance is 90-internal, 170-external
- Classless
- Support FLSM, VLSM, CIDR, Auto and Manual summary
- Metric = composite metric (32 bits)
 - - Bandwidth, load, delay, reliability
- Updates are sent as multicast(224.0.0.10) or unicast



EIGRP Features

- Incremental / triggered update
- Very fast convergence
- Max hops = 255 (default is 100 hops)
- Load balancing on 4 equal cost paths (Default)
 - Max 16 paths (equal or unequal cost paths)
- It supports multiple routed protocols
 - (IP, IPX, Apple Talk)
- EIGRP uses protocol no 88



Key Technologies of EIGRP



- Neighbor discovery
- Reliable Transport Protocol (RTP)
- DUAL Algorithm
- Protocol Dependent Modules (PDM)



EIGRP Tables



- Neighbor table
List of directly connected routers running EIGRP in same autonomous system
- Topology Table
List of all routes learned from its directly connected neighbors
- Routing table
List of best paths towards each destination



Components of EIGRP

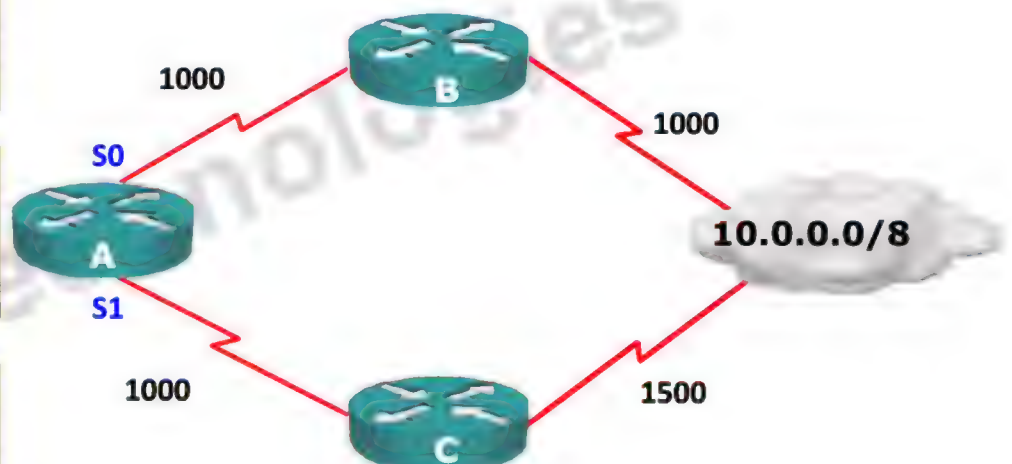
- **Link Local Distance** -- Distance from Router to Neighbor Router
- **Advertised Distance** – Distance from Neighbor Router to Destination
- **Feasible Distance** -- Link Local Distance + Advertised Distance
- **Successor** -- Best Path to reach destination
- **Feasible Successor** -- Second Best Path to reach destination

EIGRP Tables

Neighbor Table of Router A	
Neighbor	Interface
B	S0
C	S1

Topology Table of Router A				
Network	NH	AD	FD	
10.0.0.0/8	B	1000	2000	S
	C	1500	2500	

Routing Table of Router A		
Network	Next Hop	FD
10.0.0.0/8	B	2000



EIGRP metric calculation

- EIGRP Metric
- = $[K1 * BW + ((K2 * BW) / (256 - \text{load})) + K3 * \text{delay}]$



- Formula with default K values
(K1 = 1, K2 = 0, K3 = 1, K4 = 0, K5 = 0)
- EIGRP Metric
- $BW = (10^7 / \text{lowest Bandwidth in kbps}) * 256$
- $\text{Delay} = (\text{sum of total delay} / 10) * 256$

EIGRP Metrics Calculation Example



- **Delay is the sum of all the delays of the links along the paths:**
 $\text{Delay} = [\text{delay in tens of microseconds}] \times 256$
- **Bandwidth is the lowest bandwidth of the links along the paths:**
 $\text{Bandwidth} = [10,000,000 / (\text{bandwidth in kbps})] \times 256$

A → 192.168.2.0 Least bandwidth 256 kbps Total delay 41,000

Composite Metric = $[[10000000 / 256] \times 256] + [[41000 / 10] \times 256]$
= 10000000 + 1049600 = **11049600**

Hello Functions

- Neighbor Discovery
- Neighbor Formation
- Keep Alive

Update

- To exchange routing information with neighbor

Query

- Query message is generated when successor is down & Feasible Successor not available

Reply

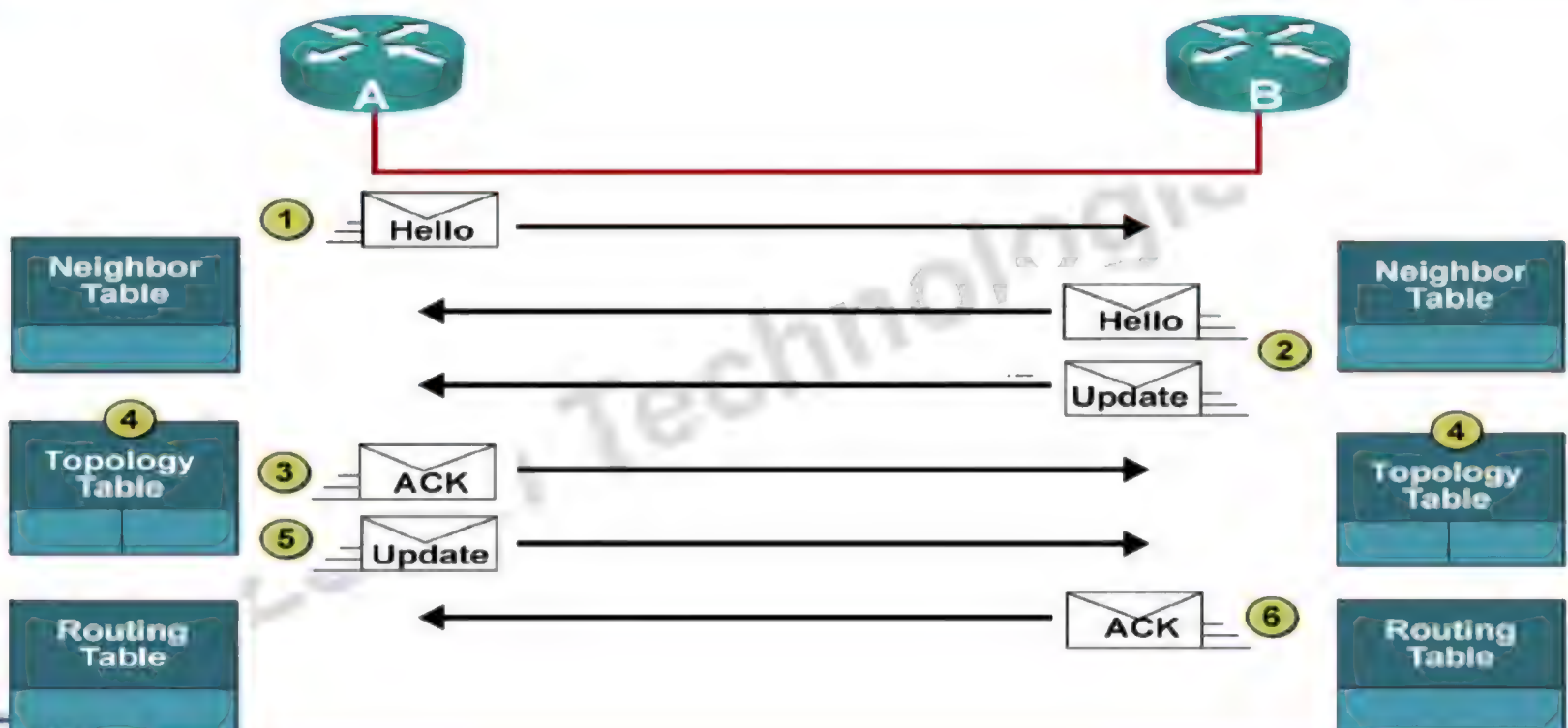
- Reply Message is sent in response to query message

ACK

- For every Update, Query and Reply router will generate ACK message



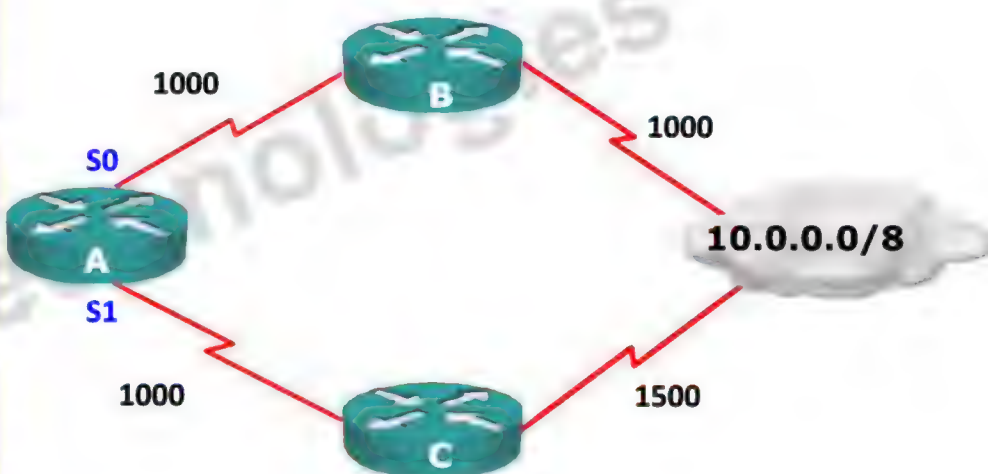
Initial Route Discovery



Neighbor Table of Router A	
Neighbor	Interface
B	S0
C	S1

Topology Table of Router A				
Network	NH	AD	FD	
10.0.0.0/8	B	1000	2000	S
	C	1500	2500	FS

Routing Table of Router A		
Network	Next Hop	FD
10.0.0.0/8	B	2000



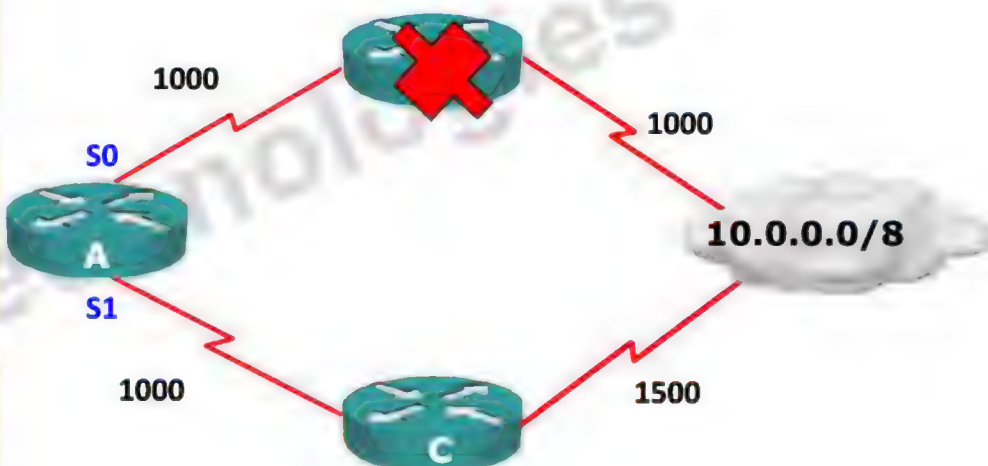
Feasibility Condition = Second best AD < FD of Successor



Neighbor Table of Router A	
Neighbor	Interface
B	S0
C	S1

Topology Table of Router A				
Network	NH	AD	FD	
10.0.0.0/8	B	1000	2000	S
	C	1500	2500	S

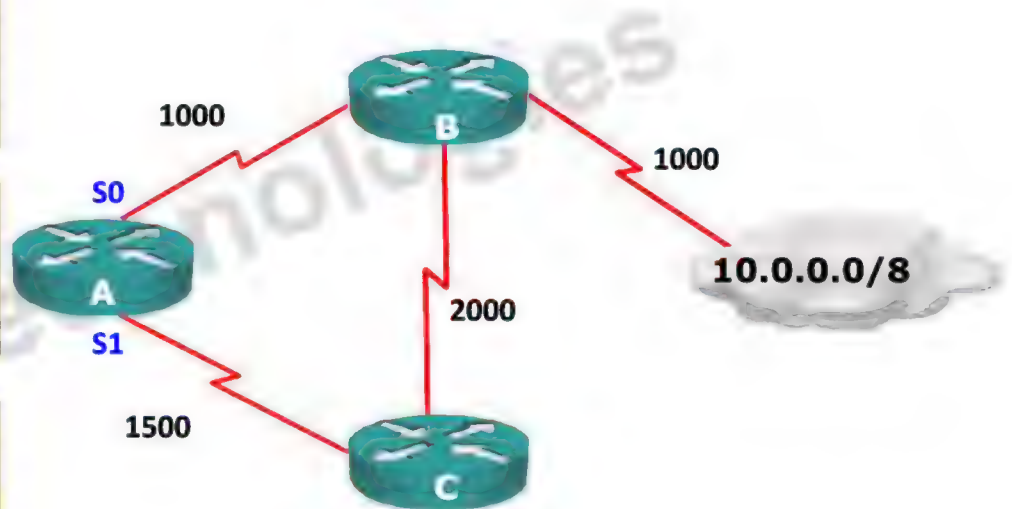
Routing Table of Router A		
Network	Next Hop	FD
10.0.0.0/8	C	2500



Neighbor Table of Router A	
Neighbor	Interface
B	S0
C	S1

Topology Table of Router A				
Network	NH	AD	FD	
10.0.0.0/8	B	1000	2000	S
	C	3000	4500	-

Routing Table of Router A		
Network	Next Hop	FD
10.0.0.0/8	B	2000



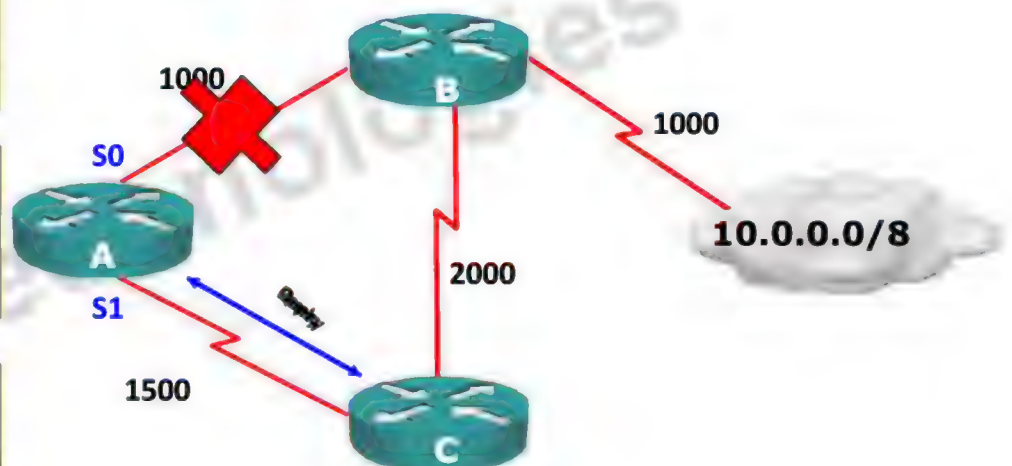
Feasible Successor = Second best AD < FD of Successor



Neighbor Table of Router A	
Neighbor	Interface
B	S0
C	S1

Topology Table of Router A				
Network	NH	AD	FD	
10.0.0.0/8	B	1000	2000	S
	C	3000	4500	S

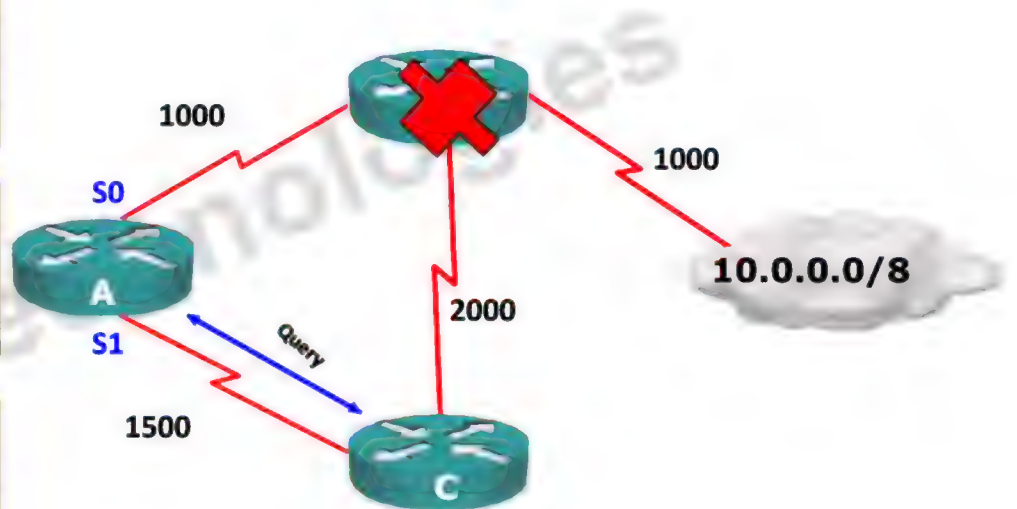
Routing Table of Router A		
Network	Next Hop	FD
10.0.0.0/8	C	4500



Neighbor Table of Router A	
Neighbor	Interface
B	S0
C	S1

Topology Table of Router A				
Network	NH	AD	FD	
10.0.0.0/8	B	1000	3000	S
	C	3000	4500	

Routing Table of Router A		
Network	Next Hop	FD
10.0.0.0/8	B	3000



Configuring EIGRP

To enable EIGRP as the IP routing protocol.

Router(config)# **router eigrp <AS No.>**

Identify attached networks participating in EIGRP.

Router(config-router)# **network network-id [wildcard-mask]**

Defining the interface's bandwidth for the purposes of Metric calculation

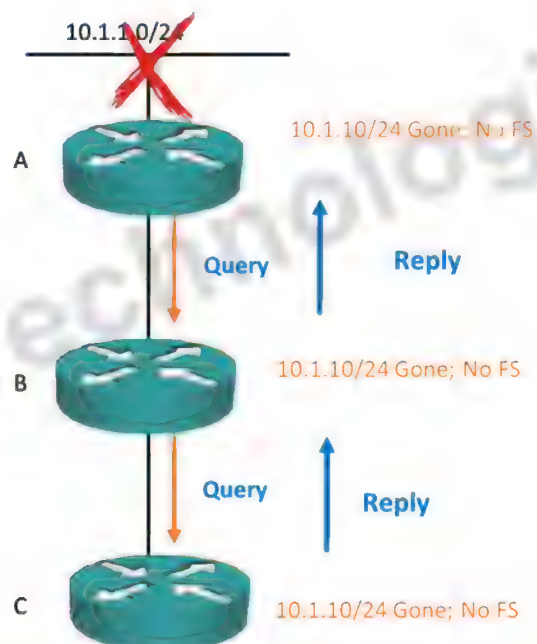
Router(config-if)# **bandwidth <kilobits>**



EIGRP Queries

- Router loses a best path and does not have a FS (Second best path) in its topology table, it looks for an alternate path to the same destination, this is called as Active state for that route.
- If a router does not have an alternate route, it queries each of its own neighbors

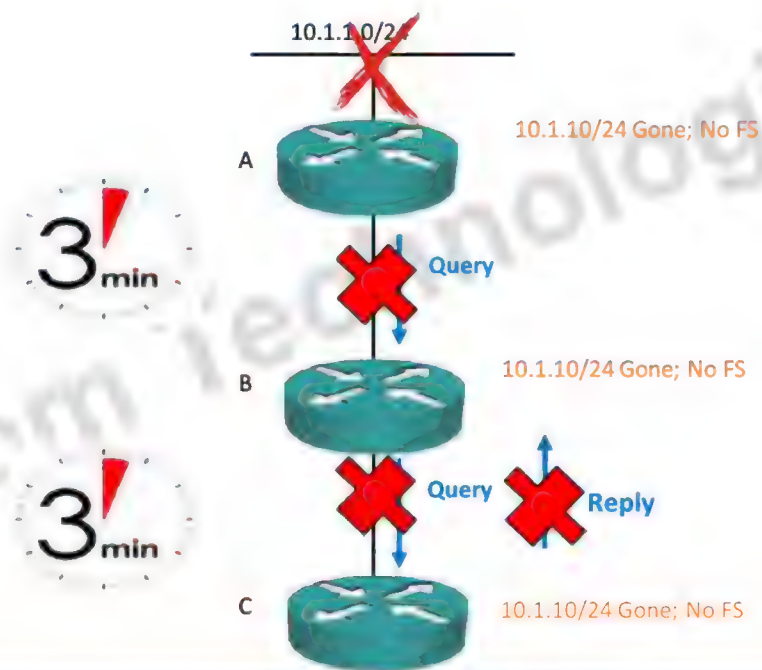
EIGRP Queries



Stuck In Active

- The most common reasons for SIA routes are as follows:
 - The router is too busy to answer the query
 - The link between the two routers is not good
 - A failure causes traffic on a link to flow in only one direction.

Stuck In Active



Preventing SIA



- Cisco IOS Software Release 12.1(5) and later, with the Active Process Enhancement feature.
- This feature enables an EIGRP router to monitor the progression of the search for a successor route and ensure that the neighbor is still reachable.

Zoom Technologies



EIGRP Stub



- EIGRP stub is a special router which will not receive Query messages.
- A stub router informs its status to all other neighbors.
- EIGRP stub routing reduces CPU utilization on the router.
- EIGRP stub routing mainly implemented in hub and spoke environment.



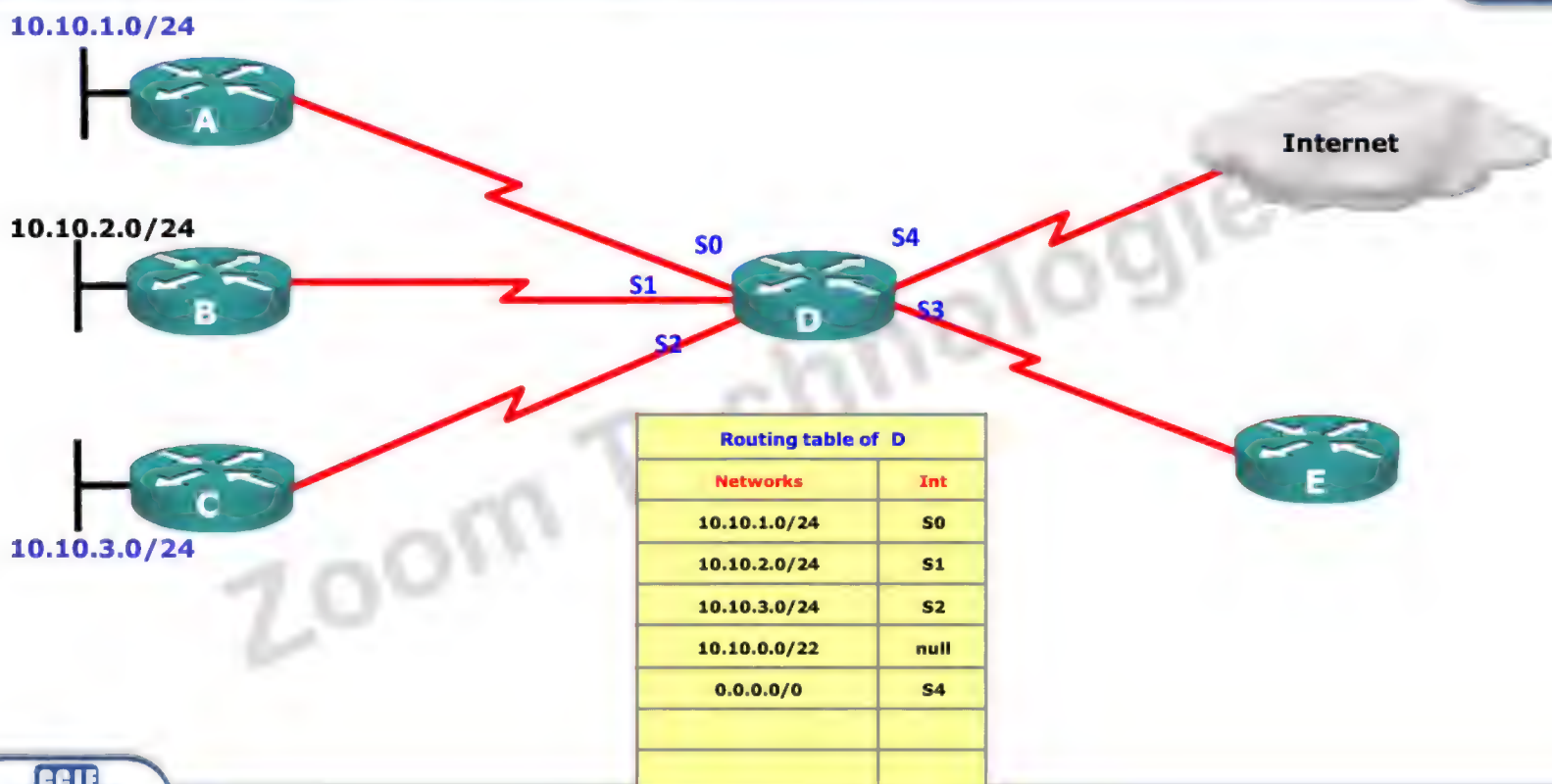
Zoom Technologies



Summarization

- Auto summary
 - EIGRP does auto summary at major logical network boundary
- Manual summary
 - EIGRP supports manual summary on a per interface basis
- Summary will be continued till the last specific route goes down
- Summary metric will be the best metric from specific route
- Router of the summary route will create a summary route pointing to null interface

Summarization with Null Interface



Configuring EIGRP Route Summarization

Turns off automatic summarization for the EIGRP process

```
Router(config-router)# no auto-summary
```

Creates a summary address that this interface will generate.

```
Router(config-if)# ip summary-address eigrp <as-number>  
                        <address> <subnet mask>
```



EIGRP Load Balancing

- Routes with lowest equal metric are installed in the routing table (equal-cost load balancing)
- There can be up to sixteen entries in the routing table for the same destination:
 - The number of entries is configurable
 - The default is four
- Variance is configured for unequal cost load balancing
 - Variance is the multiplier to FD of successor
 - Default is 1(equal cost load balancing)



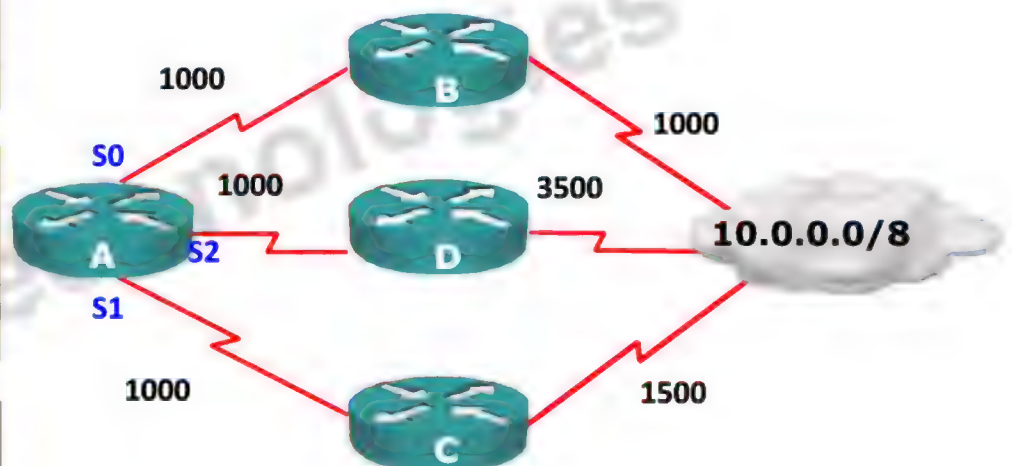
Allows the router to include routes with a metric smaller than the multiplier value times the metric of successor

Router(config-router)# variance <multiplier>

Neighbor Table of Router A	
Neighbor	Interface
B	S0
C	S1
D	S2

Topology Table of Router A				
Network	NH	AD	FD	
10.0.0.0/8	B	1000	2000	S
	C	1500	2500	FS
	D	3500	4500	-

Routing Table of Router A		
Network	Next Hop	FD
10.0.0.0/8	B	2000
	C	2500



Variance = ?

Router Authentication

- Gives greater security to the routing protocol by supporting authentication
- A router authenticates the source of each routing update packet that it receives.
- Prevent false routing updates from updating the routing table



Router Authentication

- Many routing protocols support authentication
- Router authenticates the source of each routing update
- Simple password authentication is supported by:
 - IS-IS
 - OSPF
 - RIPv2
- MD5 authentication is supported by:
 - OSPF
 - BGP
 - EIGRP




MD-5 Authentication

- MD-5 authentication uses key-chains to perform routing protocol authentication.
- Each and every Key Chain contains 1 or more keys .
- Each and Every key identified using Key number and key-string.
- Key number and key-string need to match on both the routers.



MD-5 Authentication Configuration

- Step1: Create key Chain on the router
- Router(config)# key chain zoom
- Router(config-keychain)#key 1
- Router(config-keychain-key)#key-string ccnp
- Router(config-keychain-key)#exit
- Step 2: Apply Key Chain on the Interface that is connected to neighbor
- R1(config)# key chain zoom
- R1(config-keychain)#key 1
- R1(config-keychain-key)#key-string ccnp
- R1(config-keychain-key)#exit



Open Shortest Path First (OSPF)

OSPF Features

ZOOM
TECHNOLOGIES

- Open standard (IETF)
- SPF or Dijkstra algorithm
- Link-state routing protocol
- Classless
 - Supports FLSM, VLSM, CIDR and Manual summary
- Incremental / triggered updates
- Updates are sent as multicast (224.0.0.5 and 224.0.0.6)
- Metric = Cost (cost = 108/bandwidth in bps)
- Administrative distance = 110
- Load balancing via 4 equal cost paths by default (unequal cost load balancing not supported)



Link-state Routing Protocol

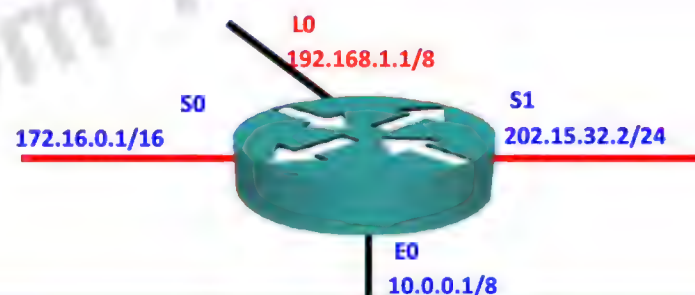
- Auto Neighbor discovery
- Hierarchical network design
- Sends periodic updates, known as link-state refresh, every 30 minutes
- Maintains similar database on all the routers within an area
- Router ID is used to identify each router

Router ID

- Highest IP address on Active Physical Interface
- Highest IP address on Logical Interface (if configured)
- Highest preference is for Router ID command

Configuring Router ID

Router(config-router)# router-id <ip address>

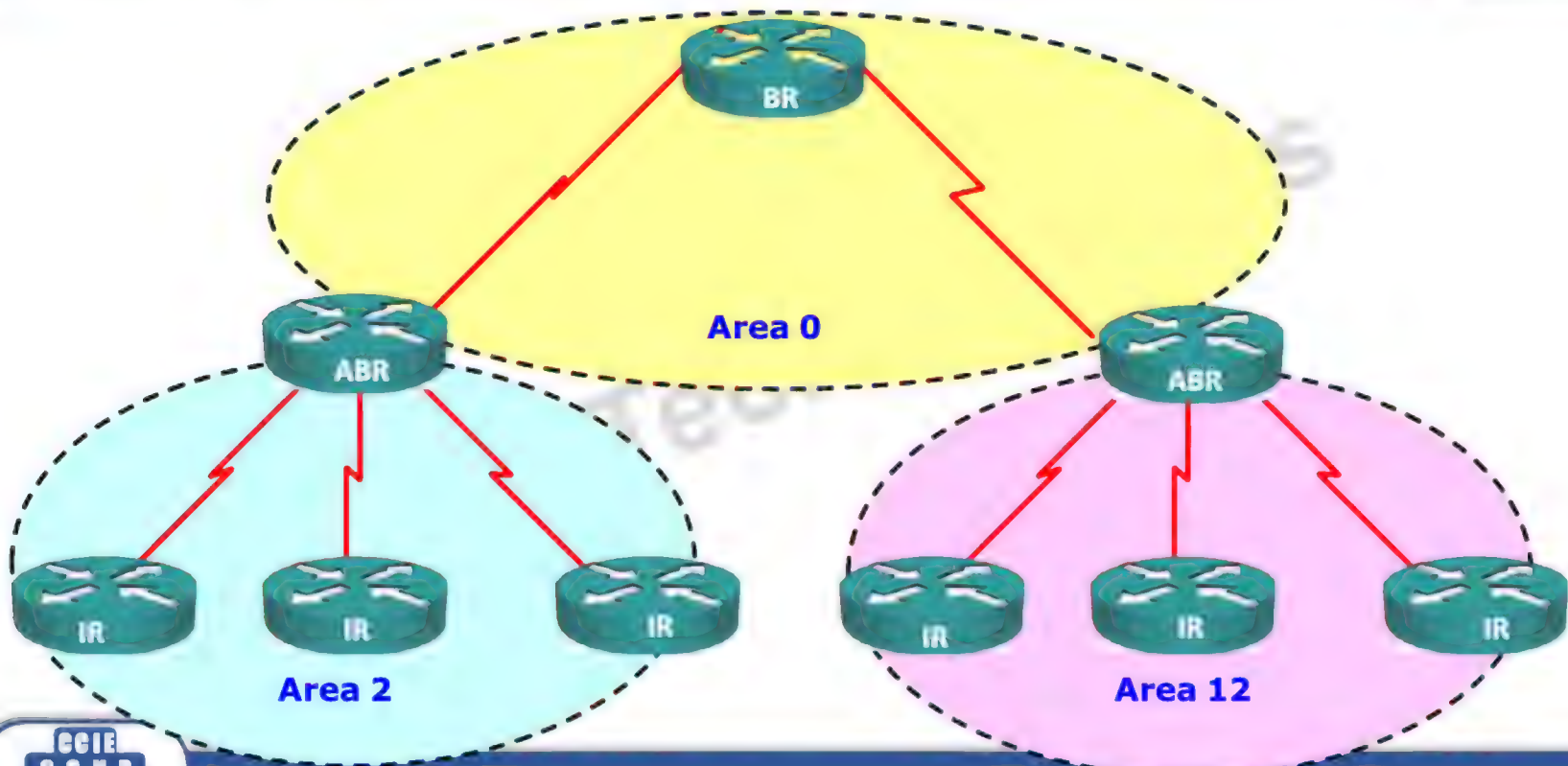


Link-State Data Structure :Network Hierarchy

- Link-state routing has a hierarchical network
- This two-level hierarchy consists of the following:
 - Transit area (backbone or area 0)
 - Regular areas (nonbackbone areas)

Zoom Technologies

OSPF Multi Area



Types of Routers in ospf



- **Backbone router-** The router which belongs to backbone area is called as Backbone router
- **Internal Router-** The router which belongs to regular area is called Internal Router
- **ABR-**The router which shares two different areas is called Area Border Router
- **ASBR-** The router which is connected to different protocol is called Autonomous system boundary router.

Zoom Technologies



Link-State Data Structures



- **Neighbor Table**
 - Also known as the adjacency database
 - Contains list of recognized neighbors
- **Database Table**
 - Typically referred to as LSDB
 - Contains information about all routers and their attached links in the area or networks
- **Routing Table**
 - Commonly named as forwarding database
 - Contains list of best paths to each destination

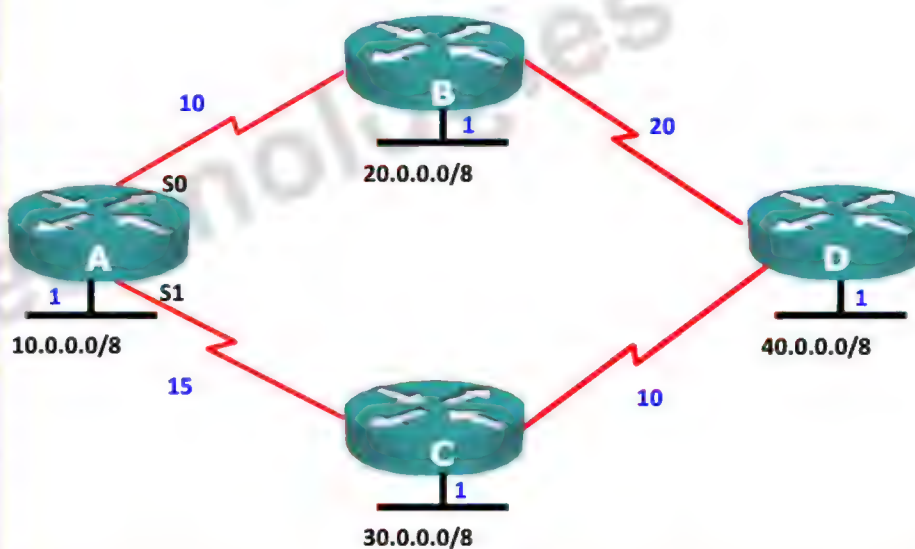
Zoom Technologies



Neighbor Table of Router A	
Neighbor	Interface
B	S0
C	S1

Link State Data base of Router A	
Router	Links
A	5
B	5
C	5
D	5

Routing Table of Router A		
Network	Next Hop	Cost
20.0.0.0/8	B	11
30.0.0.0/8	C	16
40.0.0.0/8	C	26



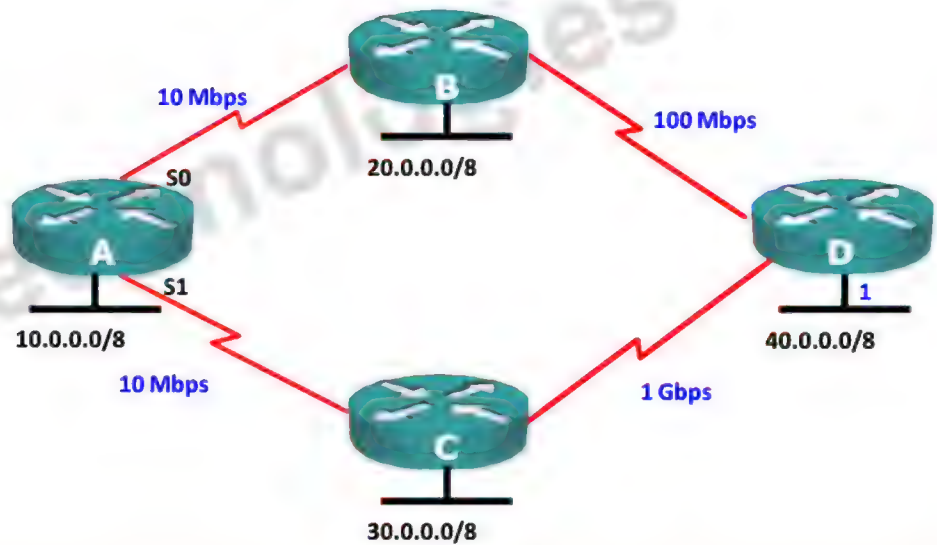
OSPF Metric calculation

- OSPF metric is not defined in standards
- Every vendor uses a different formula to calculate metric
- OSPF Metric in Cisco = Cost = $108 / \text{Bandwidth in bps}$
- Ex:

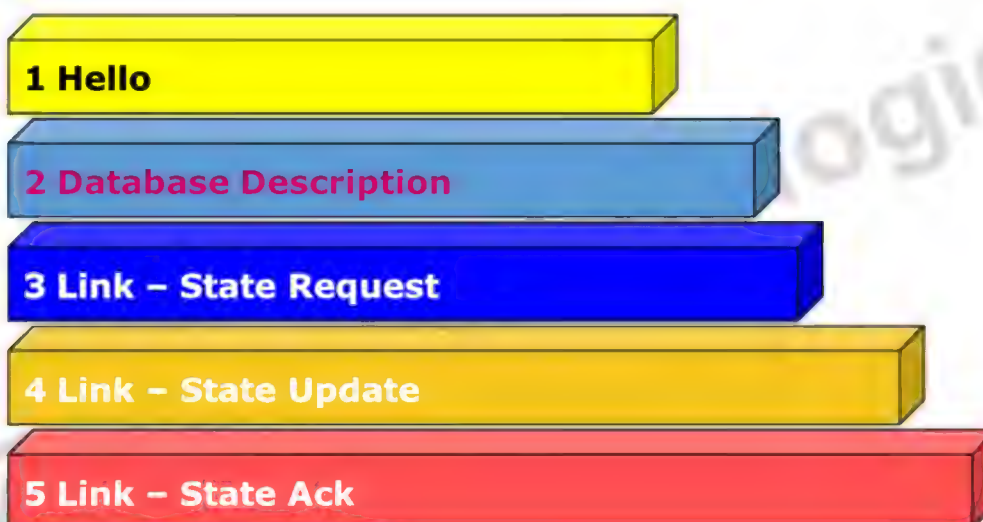
• Serial link	64 Kbps	cost = 1562
•	1544 Kbps	cost = 64
•	2000 Kbps	cost = 48
• Ethernet	10 Mbps	cost = 10
• FastEthernet	100 Mbps	cost = 1
• Gigabit Ethernet	1000 Mbps	cost = 1

OSPF Cost calculation

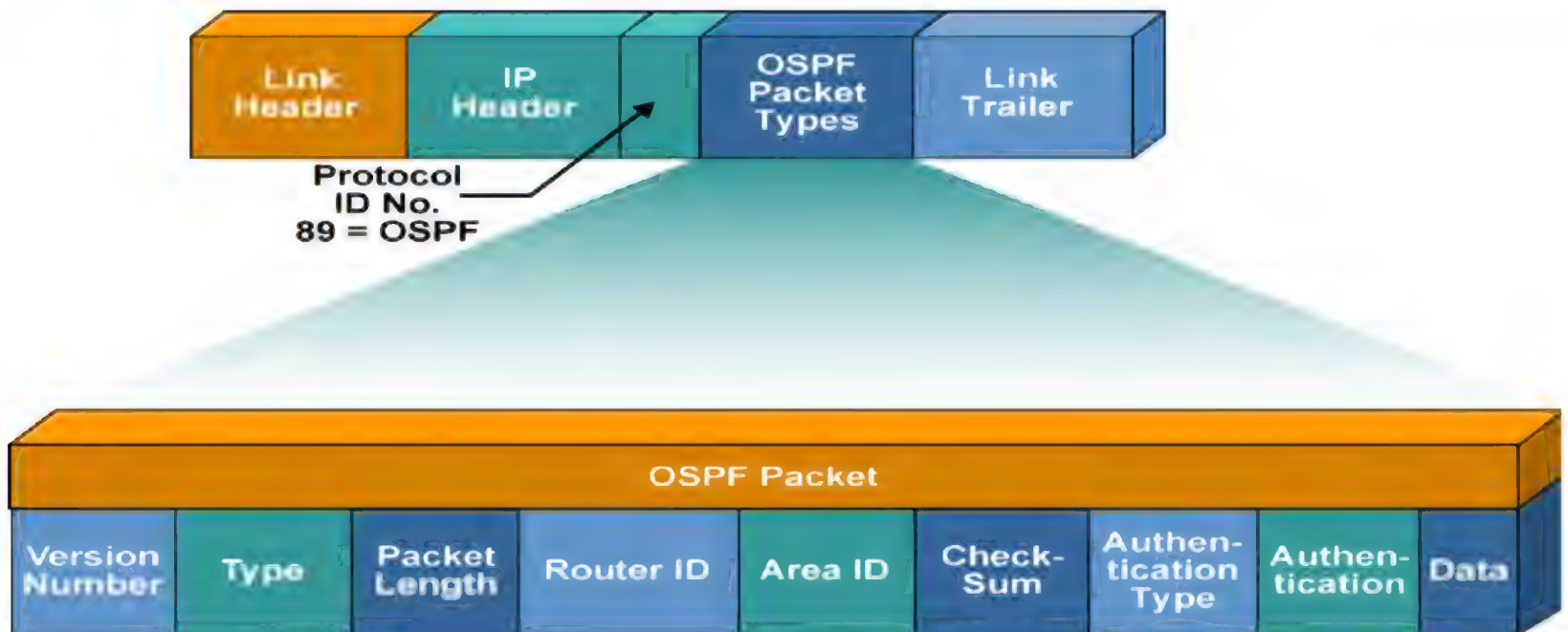
- How much does it cost to reach 40.0.0.0/8 from Router A



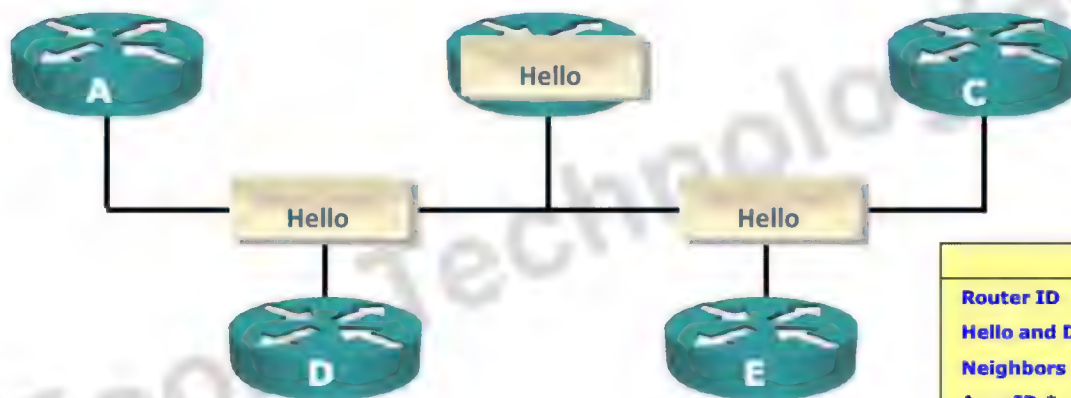
OSPF Packet Types



OSPF Packet Header Format



OSPF Neighbor relationship



HELLO
Router ID
Hello and Dead Intervals *
Neighbors
Area ID *
Router Priority
DR/BDR IP Address
Authentication Password *
Stub Area Flag *
* Entry must match on neighboring routers

Establishing bidirectional Communication

ZOOM
TECHNOLOGIES



CCNA

Establishing bidirectional Communication

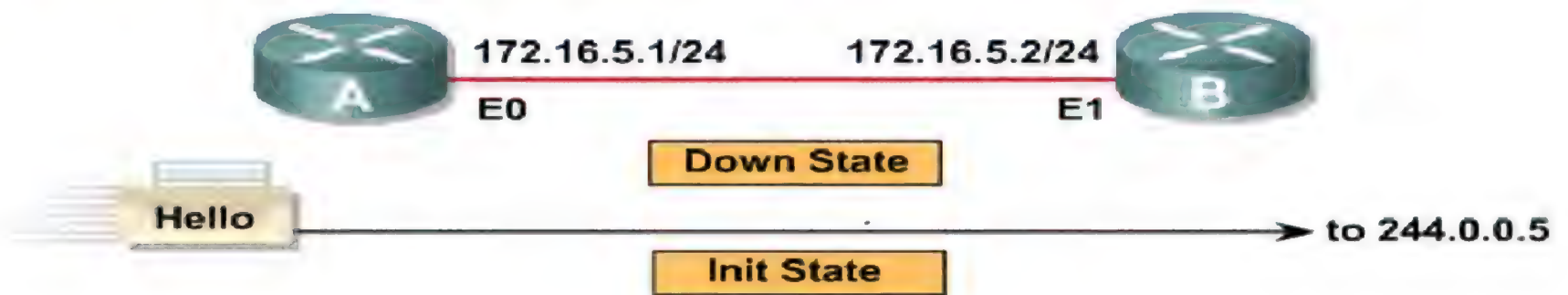
ZOOM
TECHNOLOGIES



CCNA

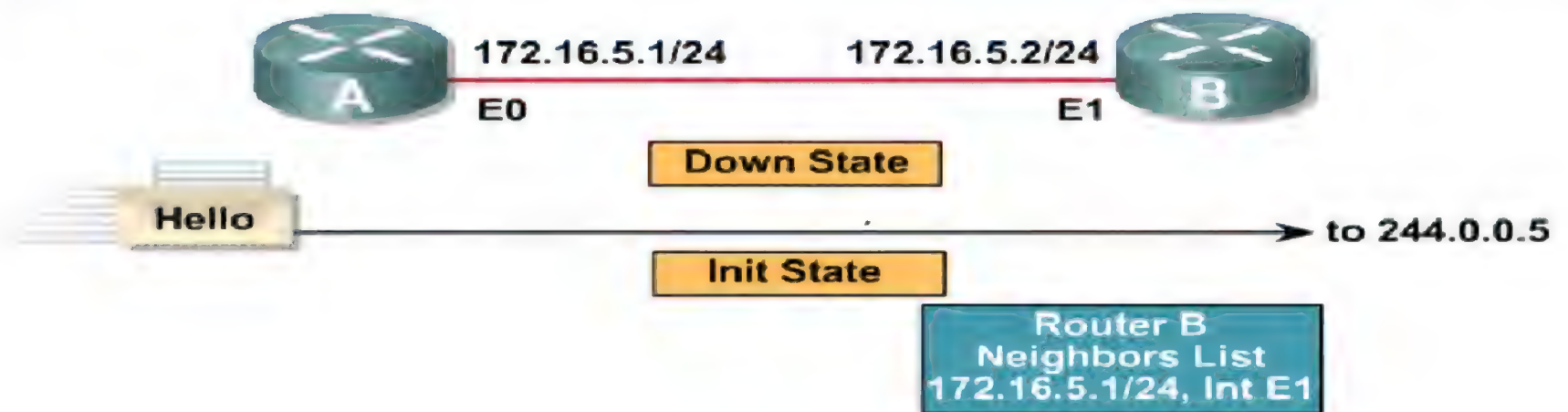
Establishing bidirectional Communication

ZOOM
TECHNOLOGIES



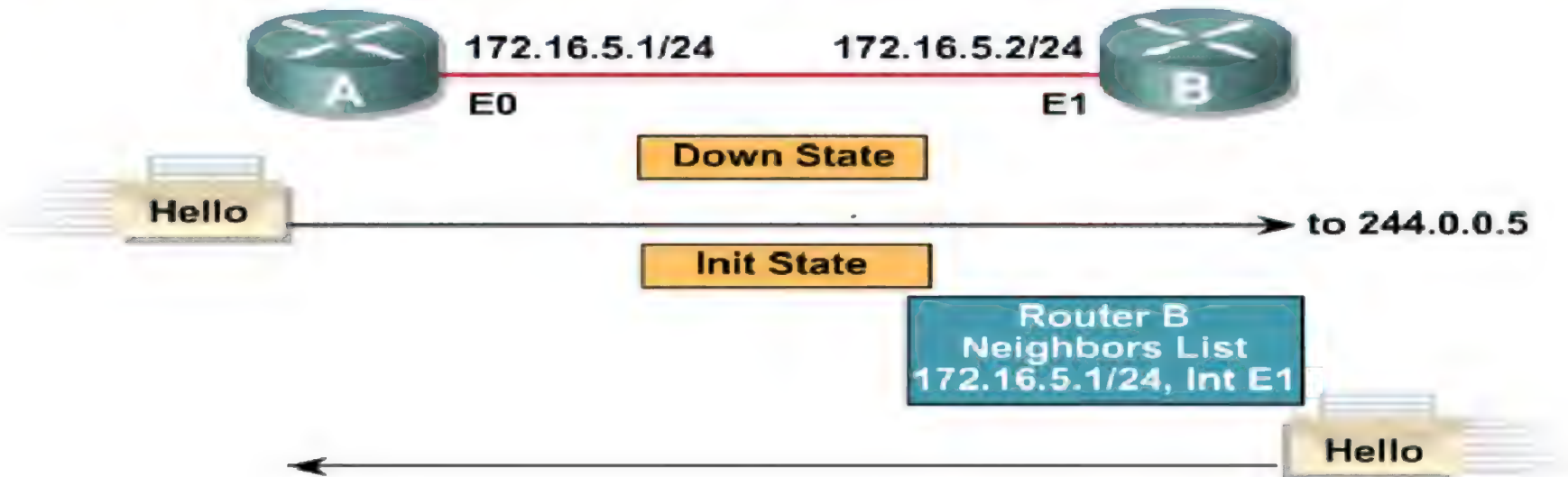
Establishing bidirectional Communication

ZOOM
TECHNOLOGIES



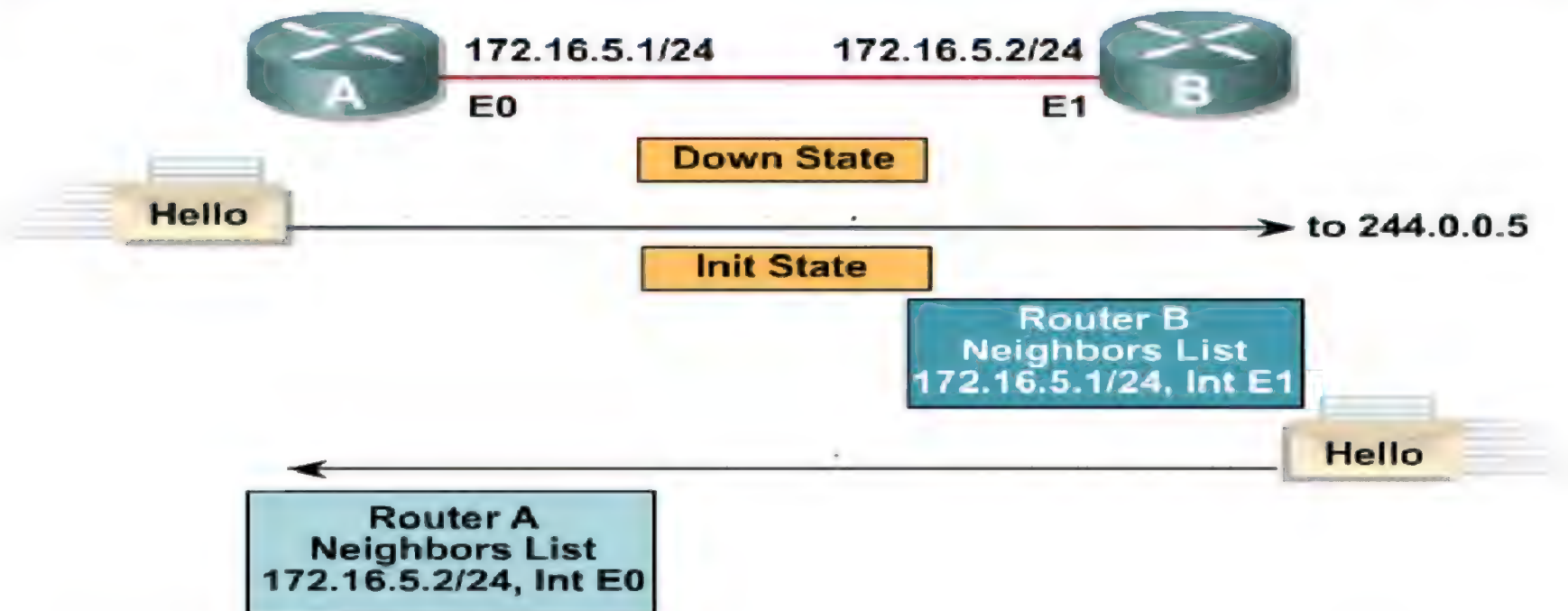
Establishing bidirectional Communication

ZOOM
TECHNOLOGIES



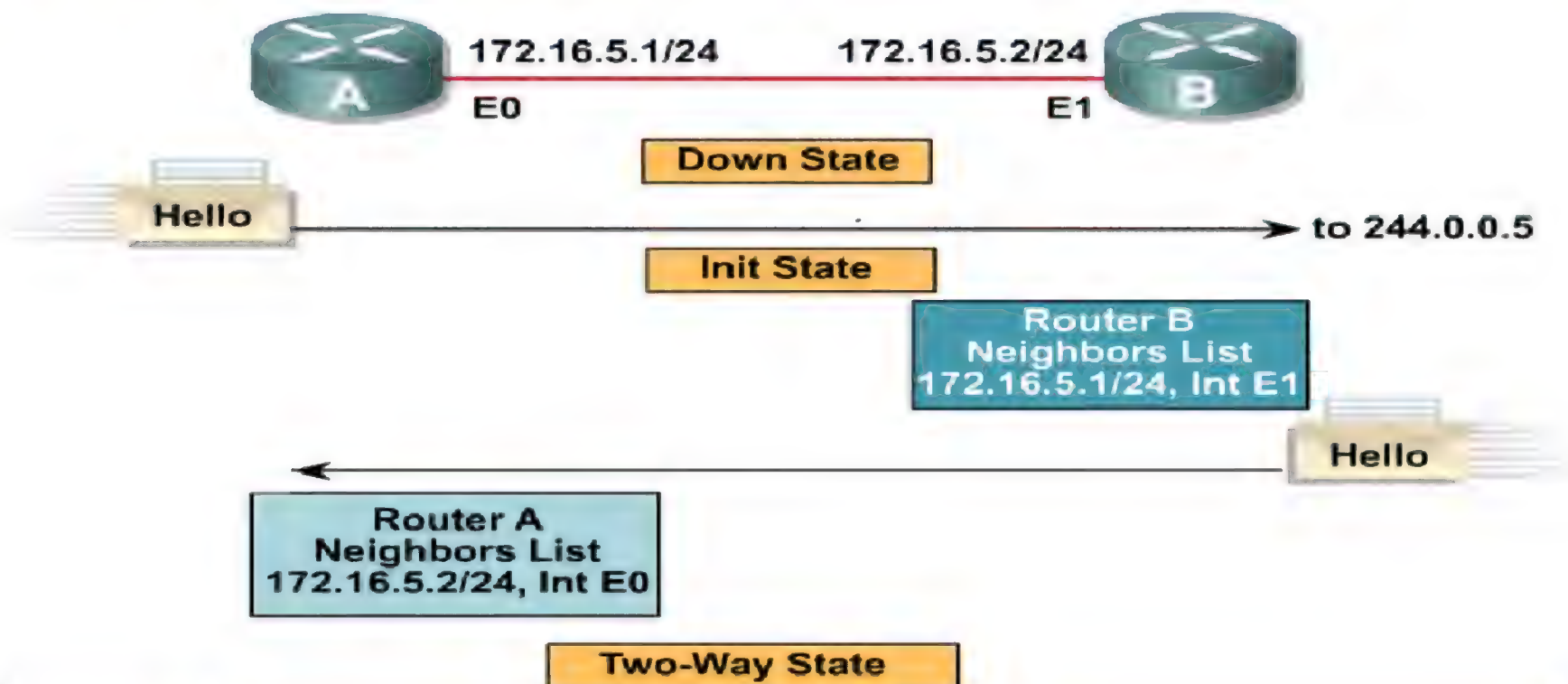
Establishing bidirectional Communication

ZOOM
TECHNOLOGIES



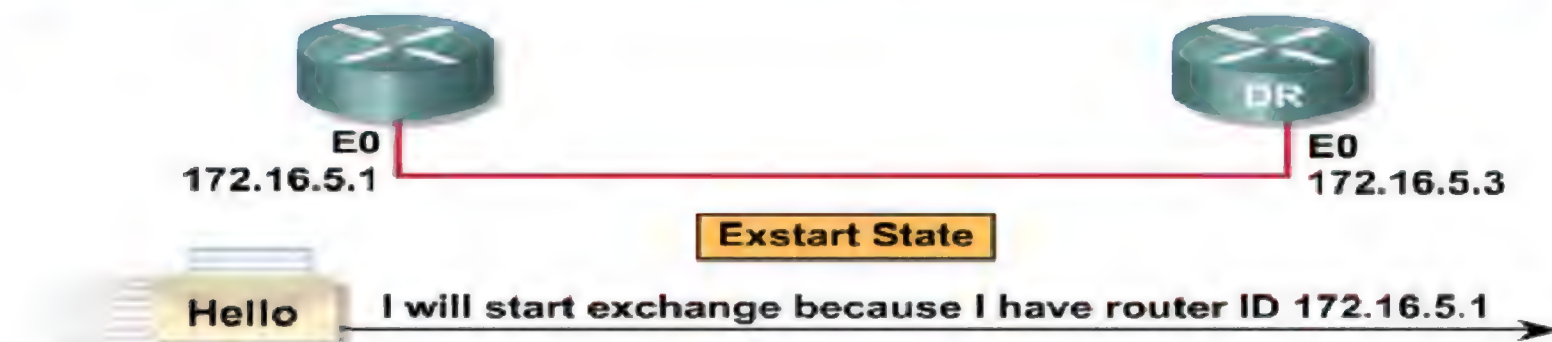
Establishing bidirectional Communication

ZOOM
TECHNOLOGIES



Establishing bidirectional Communication

ZOOM
TECHNOLOGIES



Establishing bidirectional Communication

ZOOM
TECHNOLOGIES



Exstart State

Hello

I will start exchange because I have router ID 172.16.5.1

No, I will start exchange because I have a higher router ID.

Hello

Exchange State

Establishing bidirectional Communication

ZOOM
TECHNOLOGIES



Exstart State

DBD

I will start exchange because I have router ID 172.16.5.1

No, I will start exchange because I have a higher router ID.

DBD

Exchange State

Here is a summary of my LSDB.

DBD

Establishing bidirectional Communication

ZOOM
TECHNOLOGIES



Exstart State

Hello

I will start exchange because I have router ID 172.16.5.1

No, I will start exchange because I have a higher router ID.

Hello

Exchange State

Here is a summary of my LSDB.

DBD

DBD

Here is a summary of my LSDB.

CCNA

Establishing bidirectional Communication

ZOOM
TECHNOLOGIES



LSAck

Thanks for the information!

LSAck

CCNA

Establishing bidirectional Communication

ZOOM
TECHNOLOGIES



LSAck

Thanks for the information!

Loading State

LSAck

Establishing bidirectional Communication

ZOOM
TECHNOLOGIES



LSAck

Thanks for the information!

Loading State

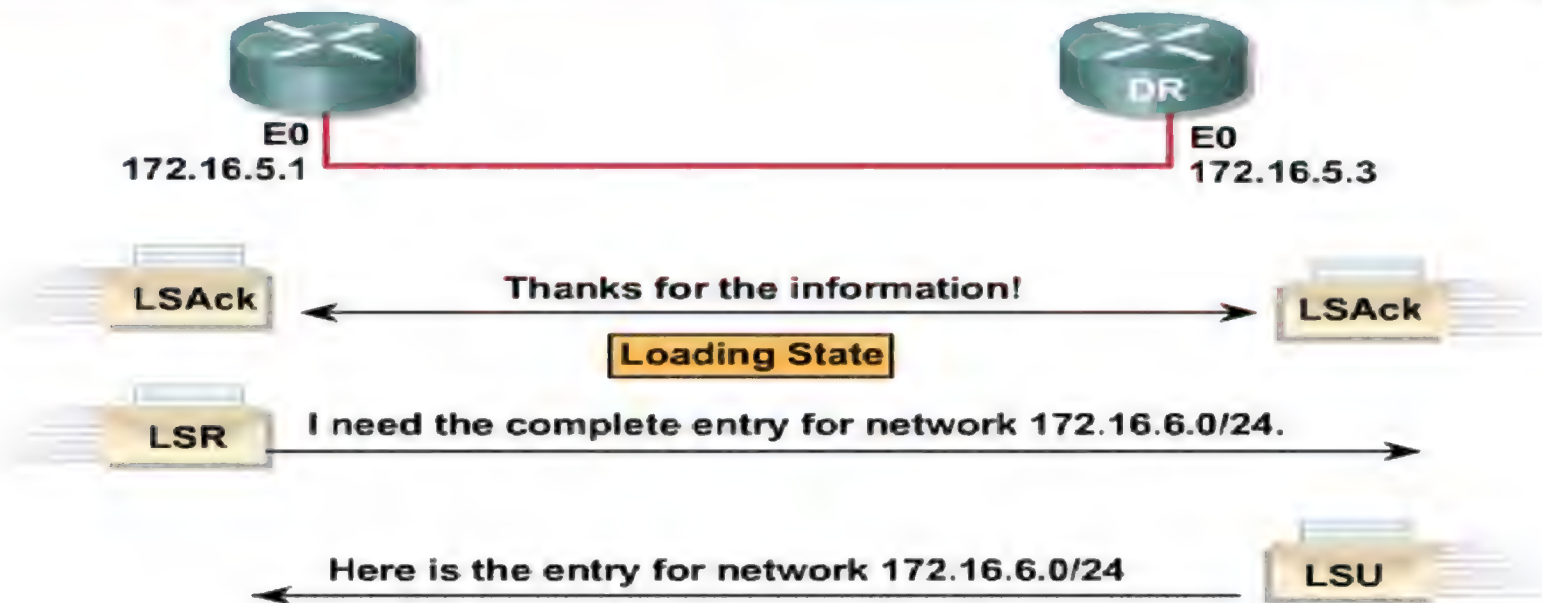
LSAck

LSR

I need the complete entry for network 172.16.6.0/24.

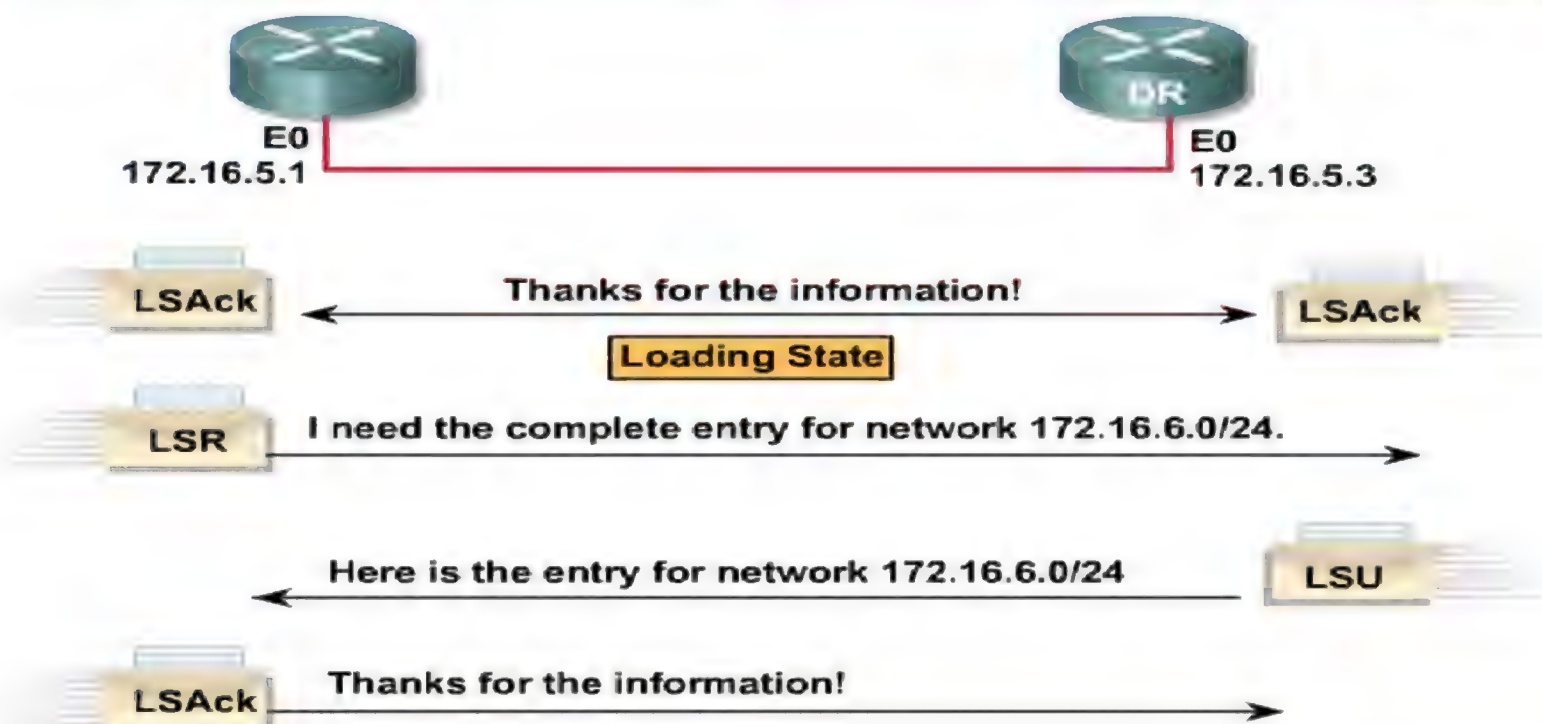
Establishing bidirectional Communication

ZOOM
TECHNOLOGIES



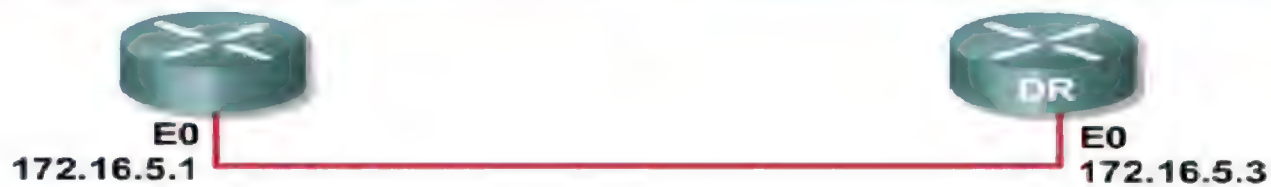
Establishing bidirectional Communication

ZOOM
TECHNOLOGIES



Establishing bidirectional Communication

ZOOM
TECHNOLOGIES



LSAck

Thanks for the information!

Loading State

LSAck

LSR

I need the complete entry for network 172.16.6.0/24.

Here is the entry for network 172.16.6.0/24

LSU

LSAck

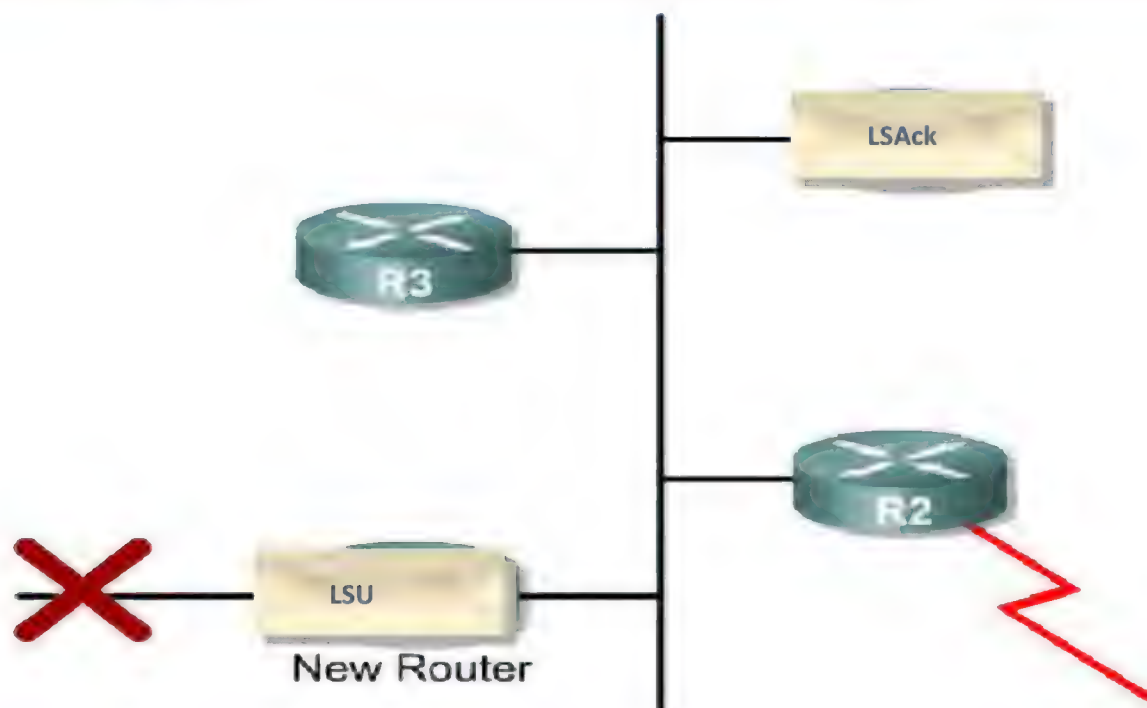
Thanks for the information!

Full State



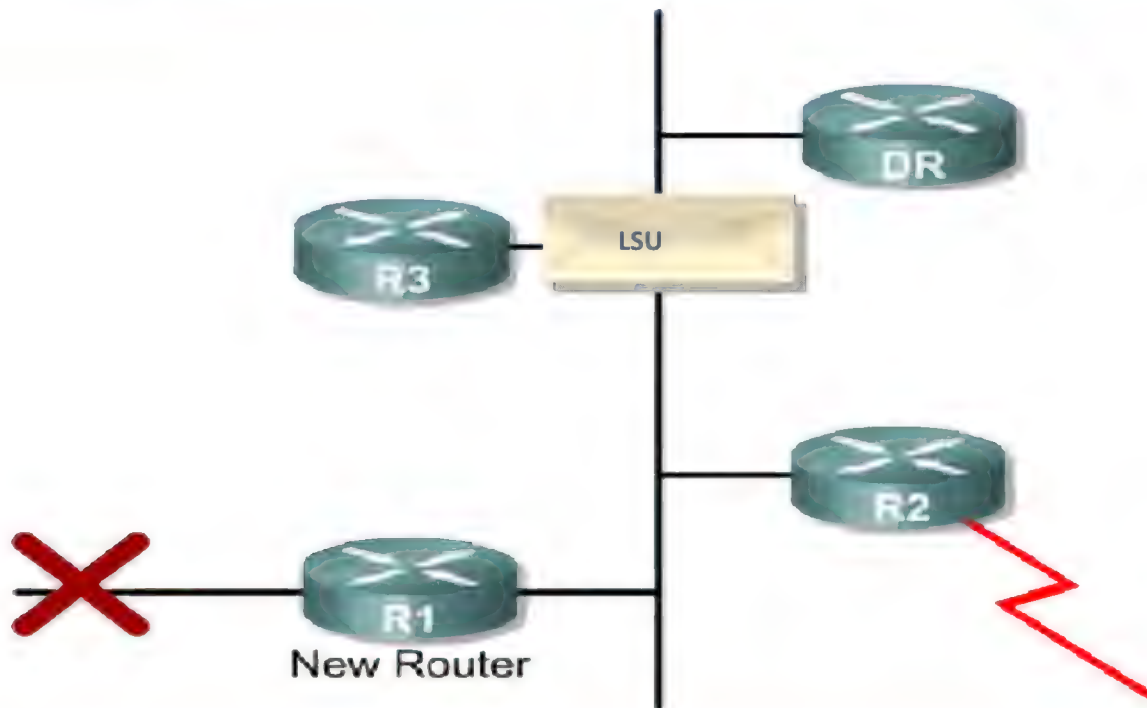
Link State Updates

ZOOM
TECHNOLOGIES



Link State Updates

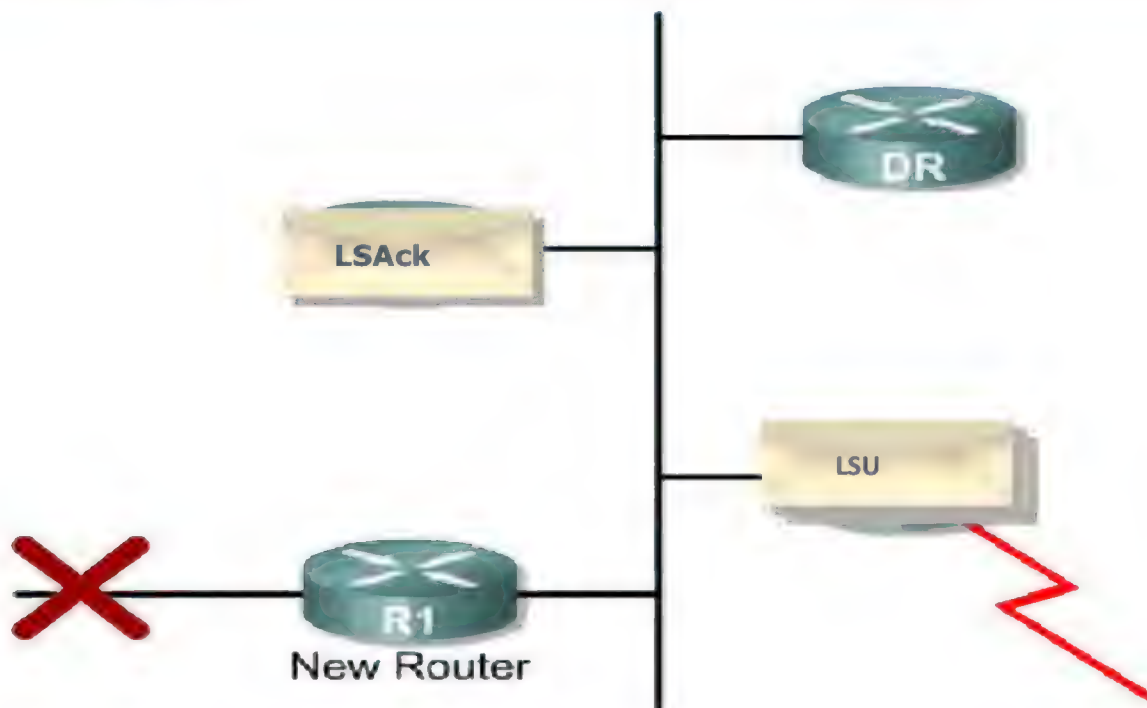
ZOOM
TECHNOLOGIES



CCIE
CCNP
CCNA

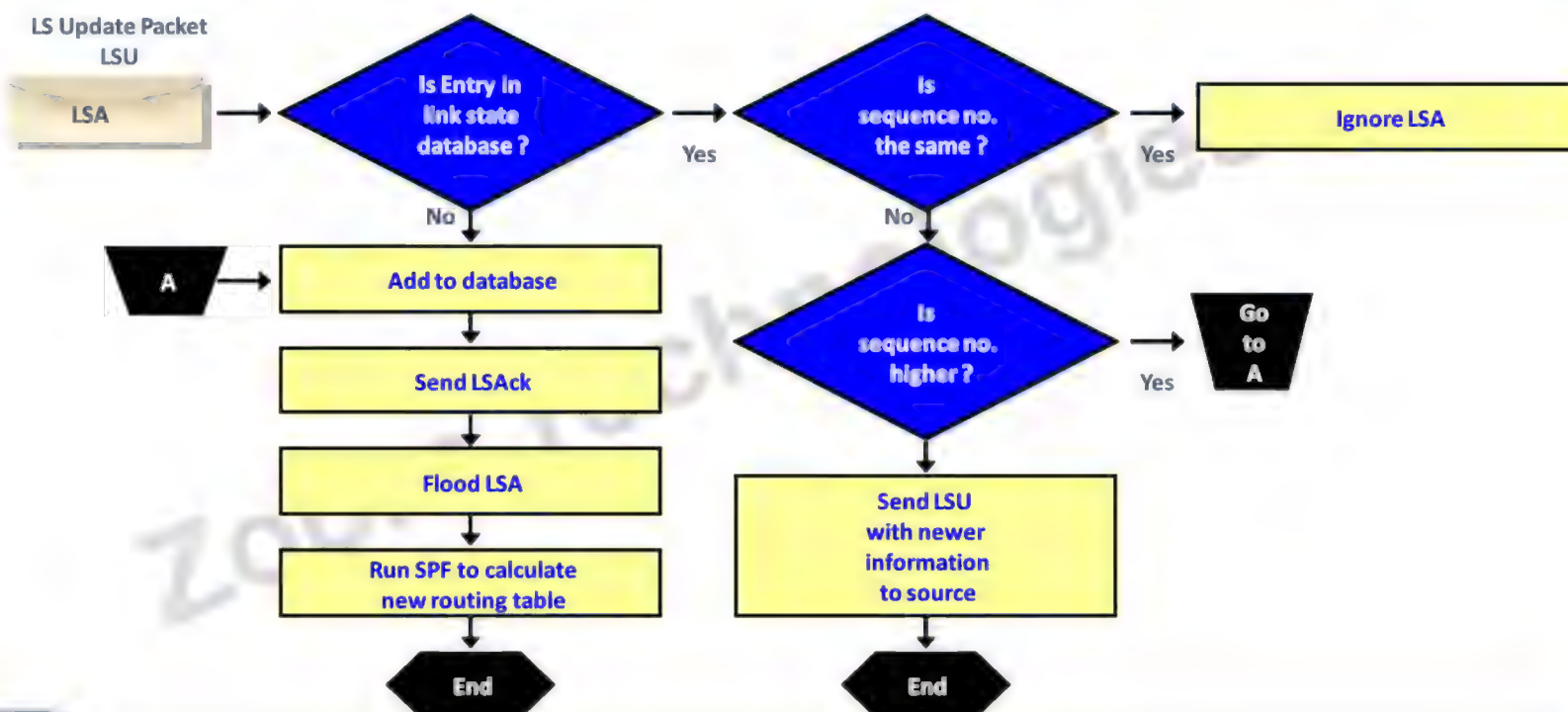
Link State Updates

ZOOM
TECHNOLOGIES



CCIE
CCNP
CCNA

LS Data Structures: LSA Operation



OSPF Network Types

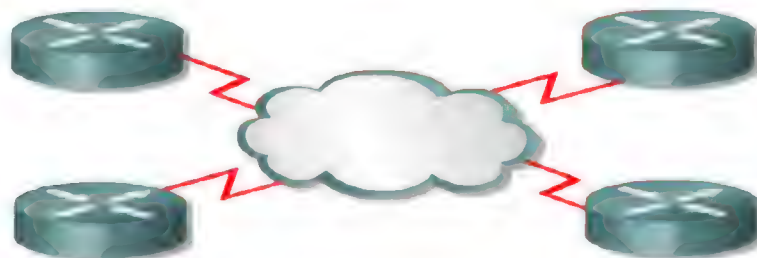
Broadcast Multiaccess



Point-to-Point

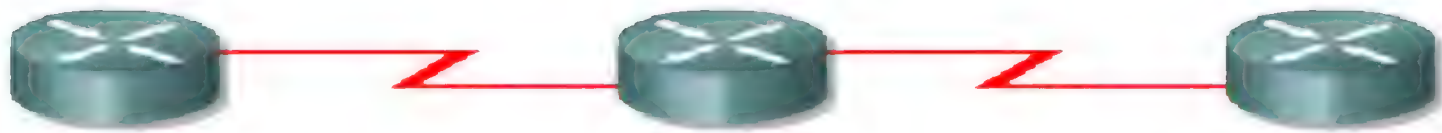


NBMA



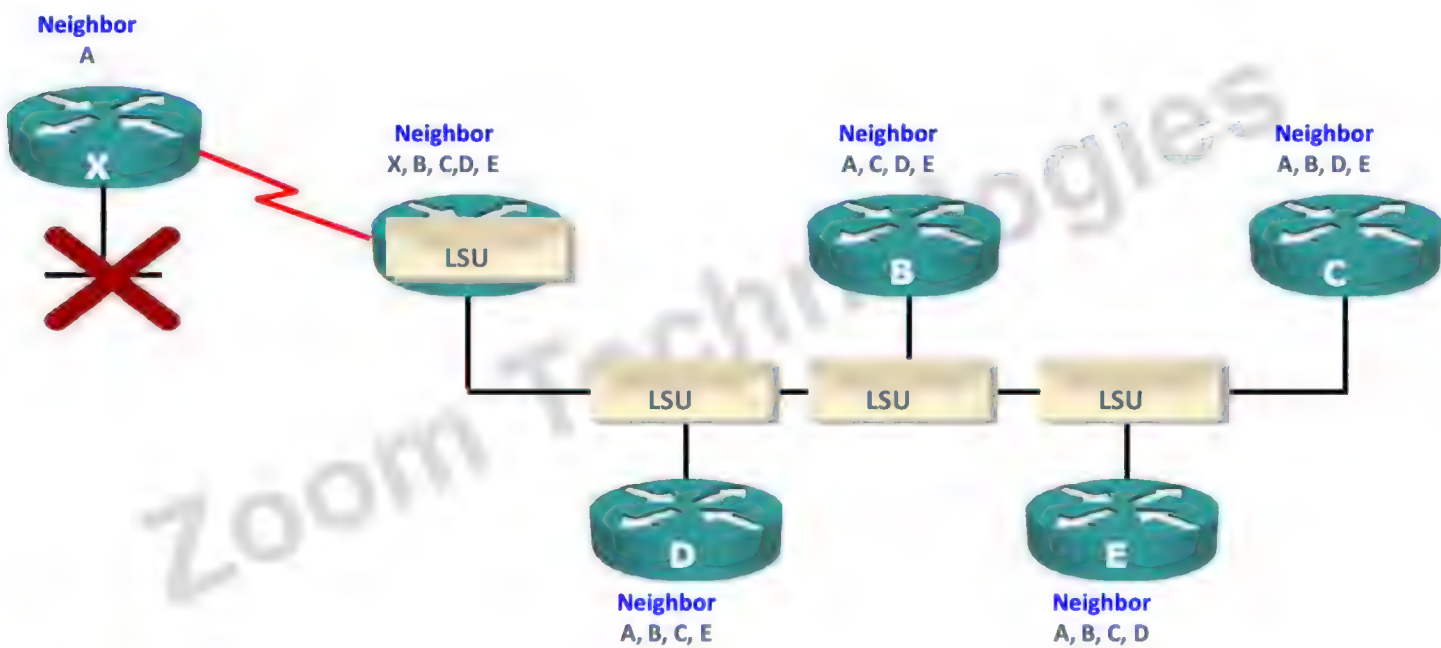
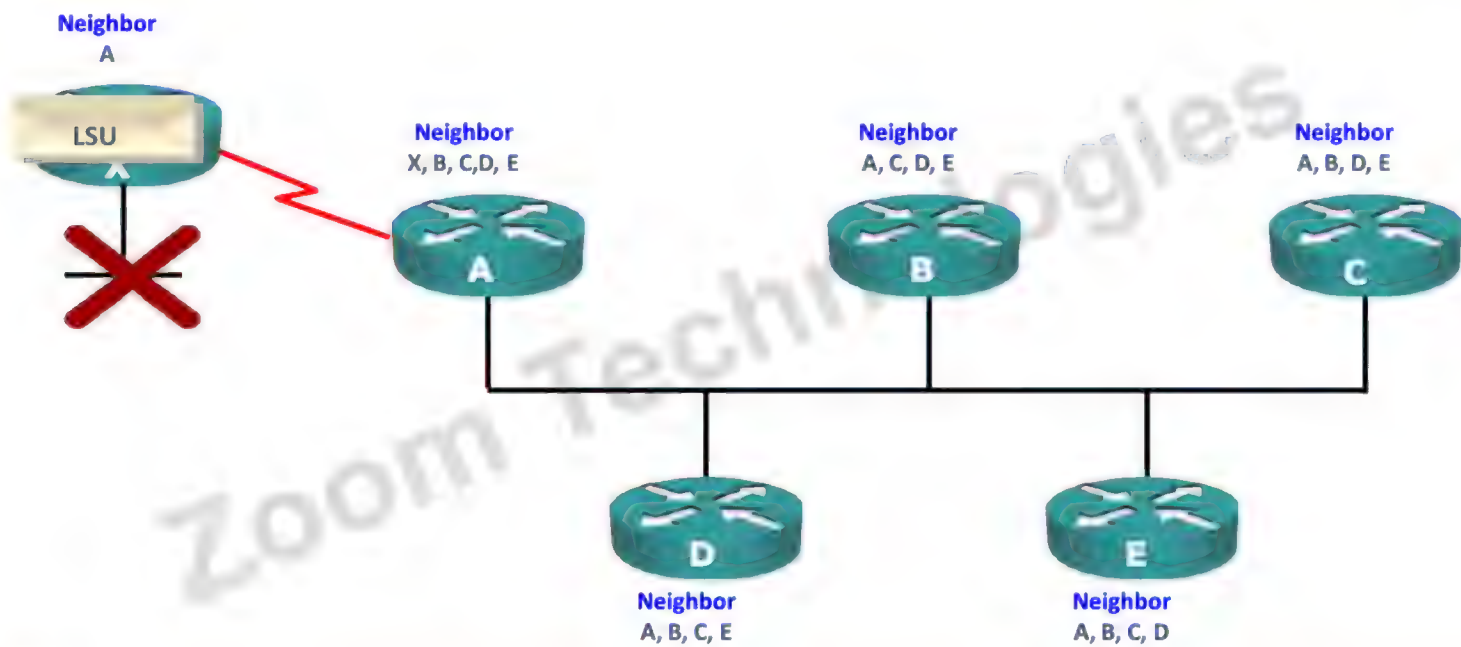
Adjacency Behavior for a Point-to-Point Link

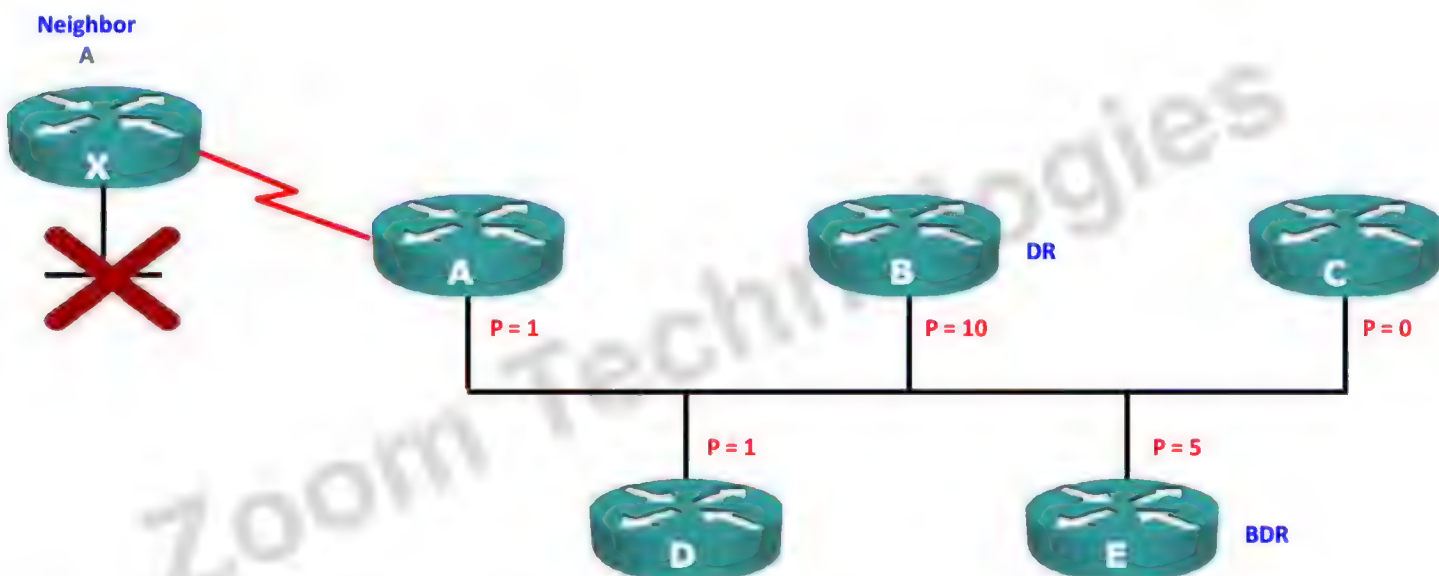
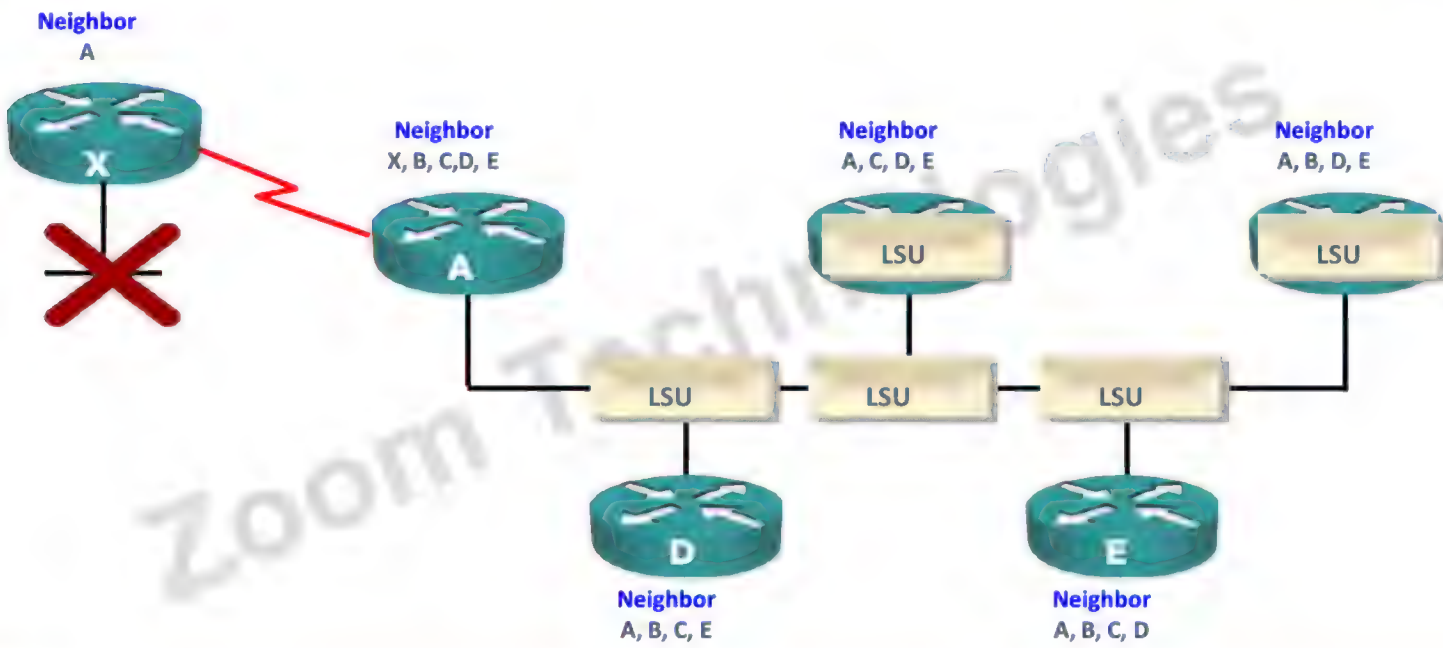
- A point-to-point link is a single pair of routers.
- Serial line configured with PPP or HDLC protocol.
- No DR or BDR election is required
- OSPF detects this type of link automatically.



Broadcast Multi Access

- Topology like Ethernet and Token Ring is BMA.
- DR and BDR Election is required.
- OSPF detects this type of link automatically



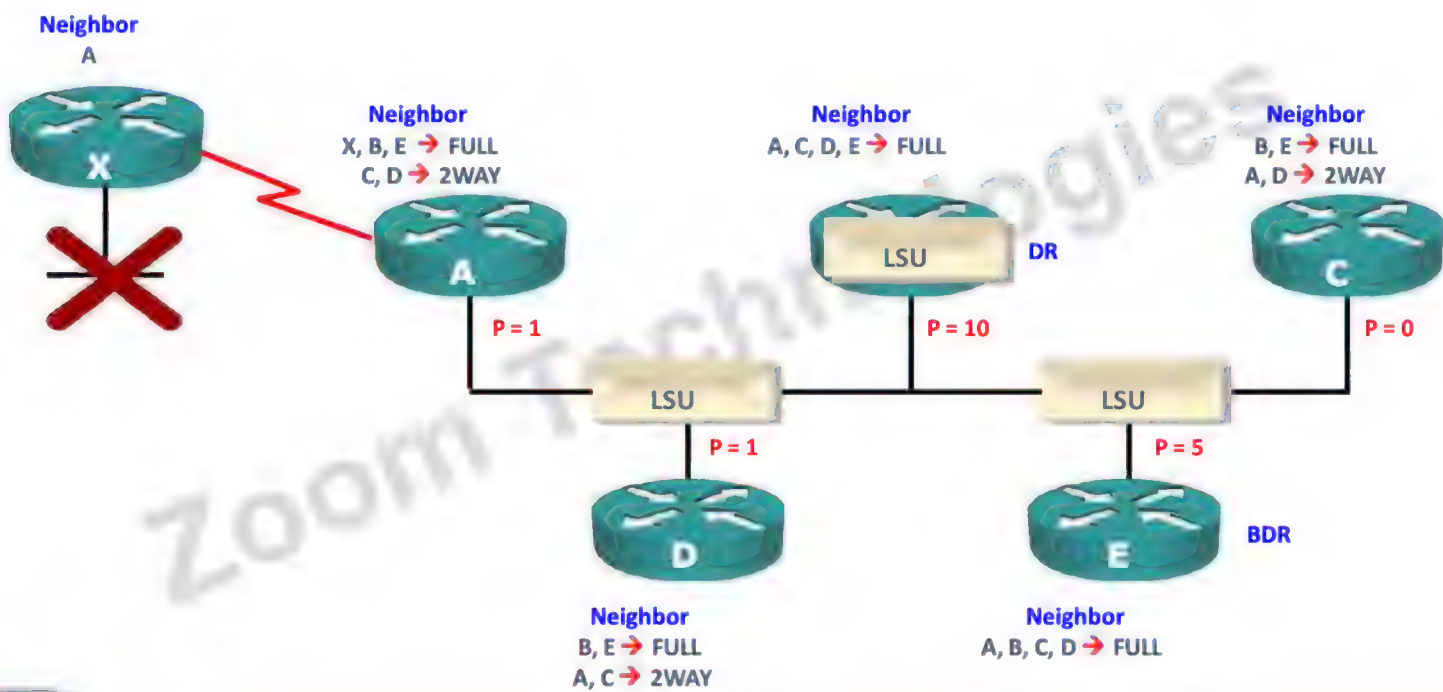
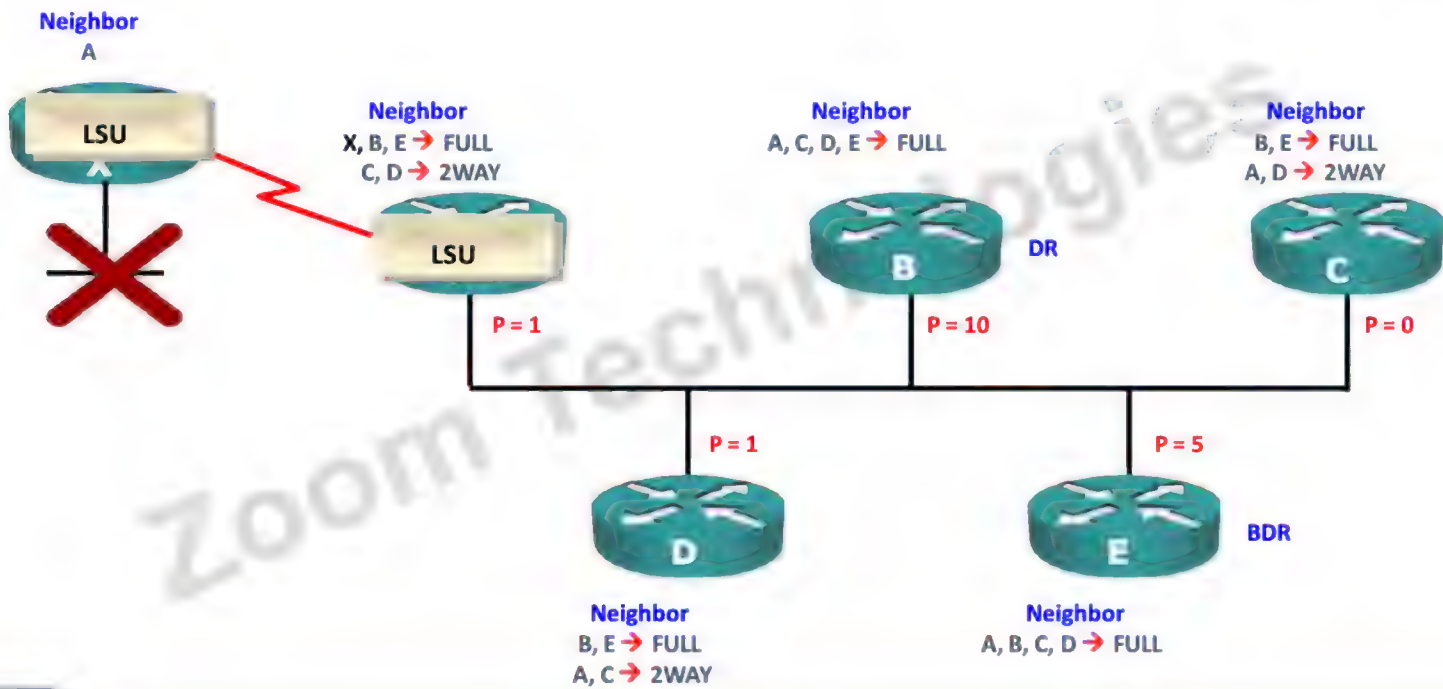


Designated Router and Backup Designated Router

- The router with the highest priority is DR
- The router with second-highest priority is BDR
- The default priority value is 1
- In the case of a tie, the router with highest router ID becomes DR , the second highest router ID becomes the BDR
- If router priority is 0 it cannot become the DR or BDR
- Router which is not a DR or BDR is called as DROTHER
- DR and BDR election is not preemptive
- We can manually set the priority to force a router to become the DR.

DR/BDR Elections

- Neighbors
- DR/BDR → DROTHER → Full
- DROTHER → DR/BDR → Full
- DROTHER → DROTHER → 2 Way
- Updates
- DROTHER → DR/BDR → 224.0.0.6
- DR → DROTHER → 224.0.0.5



NBMA

- Links like Frame relay, ATM and X.25.
- OSPF considers NBMA as other broadcast media.
- NBMA is not always full-mesh
- DR BDR election depends on type of connection.



NBMA Types

OSPF Mode	Adjacency	Configured	Hello Timer	RFC or Cisco
Broadcast	DR/BDR	Automatic	10 sec	Cisco
Nonbroadcast (NBMA)	DR/BDR	Manual	30 sec	RFC
Point-to-Multipoint	No DR/BDR	Automatic	30 sec	RFC
Point-to-Multipoint Nonbroadcast	No DR/BDR	Manual	30 sec	Cisco
Point-to-Point	No DR/BDR	Automatic	10 sec	Cisco



Open Shortest Path First (OSPF II)

Why Multiarea OSPF?

ZOOM
TECHNOLOGIES

- Single-area OSPF is useful in smaller networks. If an area becomes too big, the following issues must be addressed:
- Large routing table
- Large link-state database (LSDB)
- Frequent SPF algorithm calculations

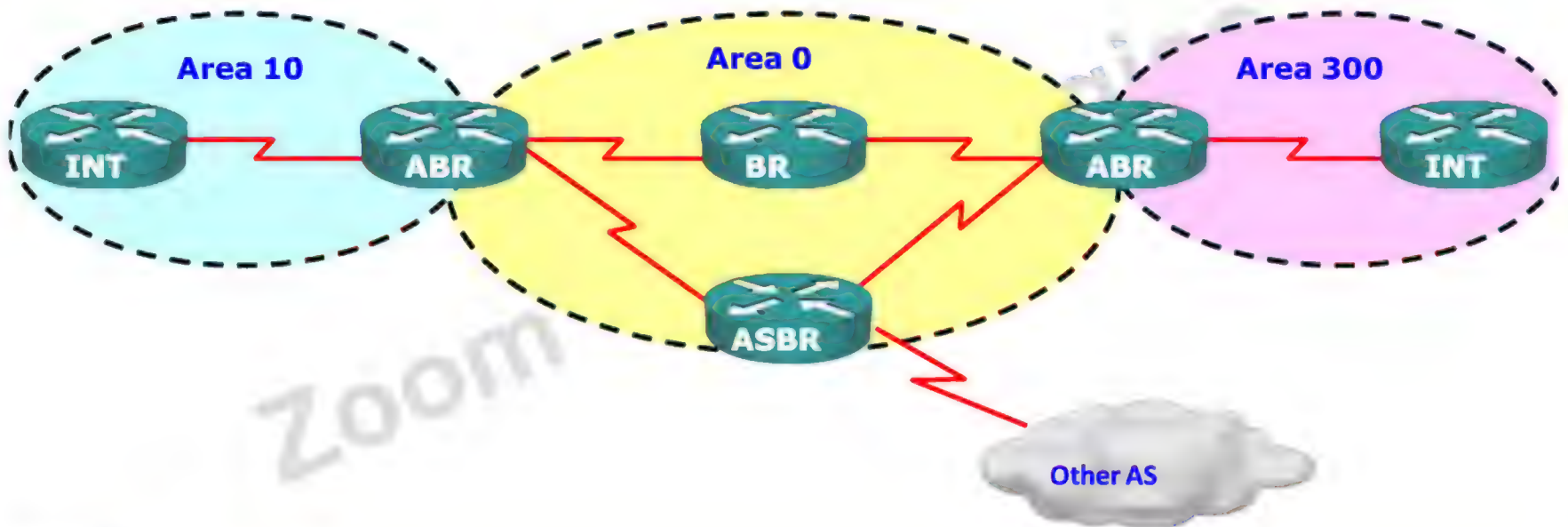


Multi Area OSPF

Multiarea OSPF requires a hierarchical network design and the main area is called the backbone area, or area 0, and all other areas must connect to the backbone area.



Type of OSPF Routers





OSPF Summarization

Benefits Of Route Summarization

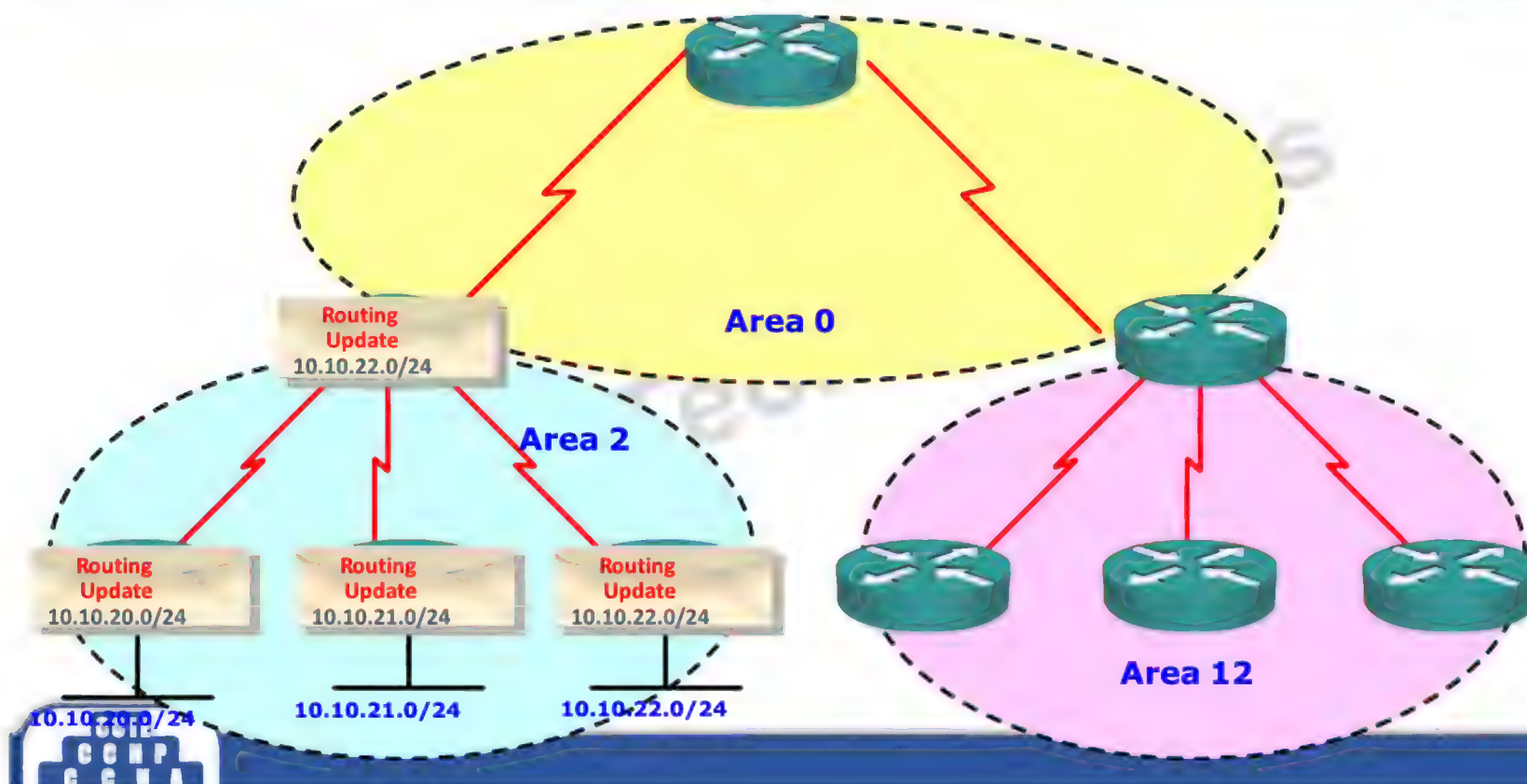
ZOOM
TECHNOLOGIES

- Minimizes number of routing table entries
- Localizes the impact of a topology change
- Reduces LSA 3 and 5 flooding and saves CPU resources

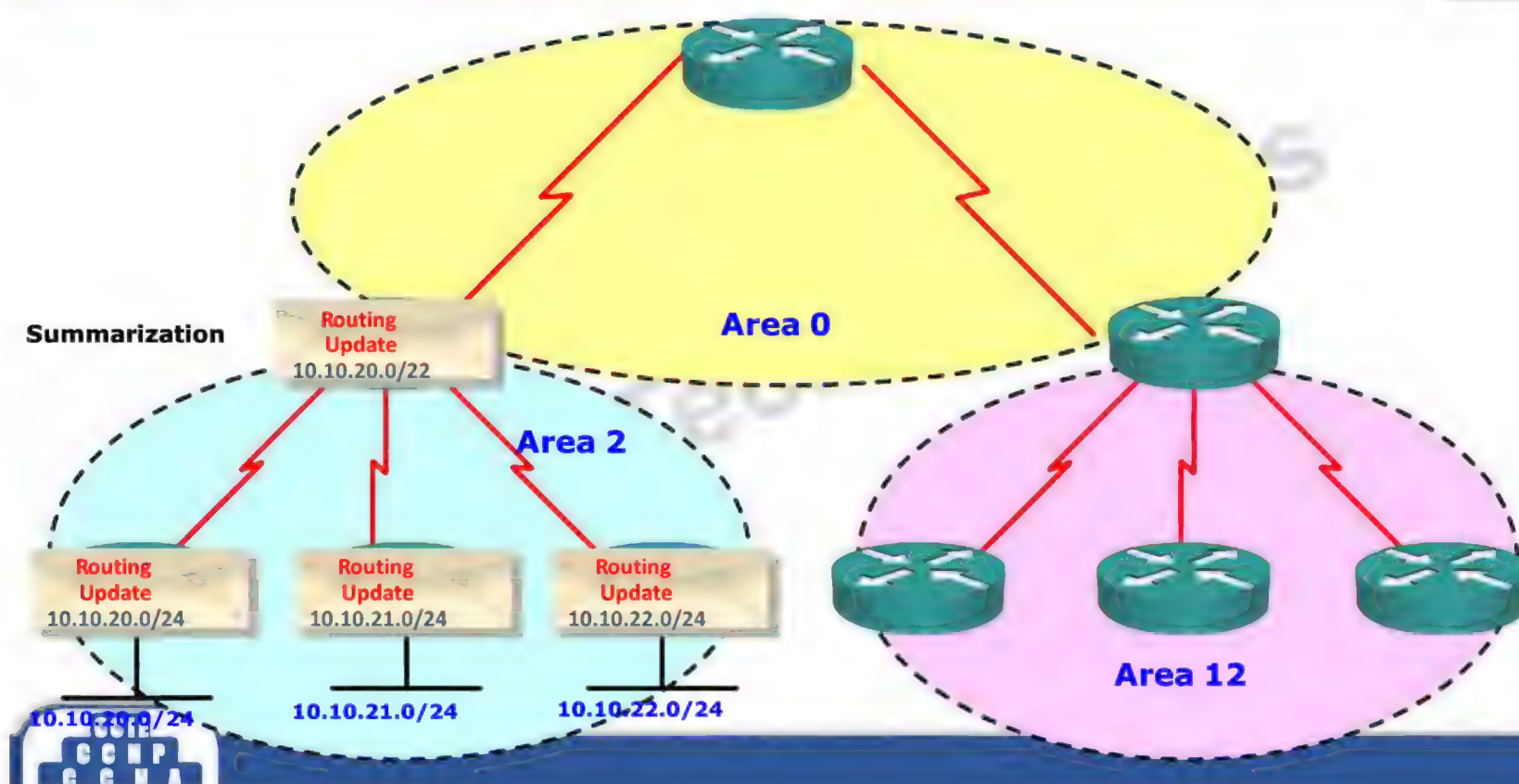
Zoom Technologies



Before Route Summarization



After Route Summarization



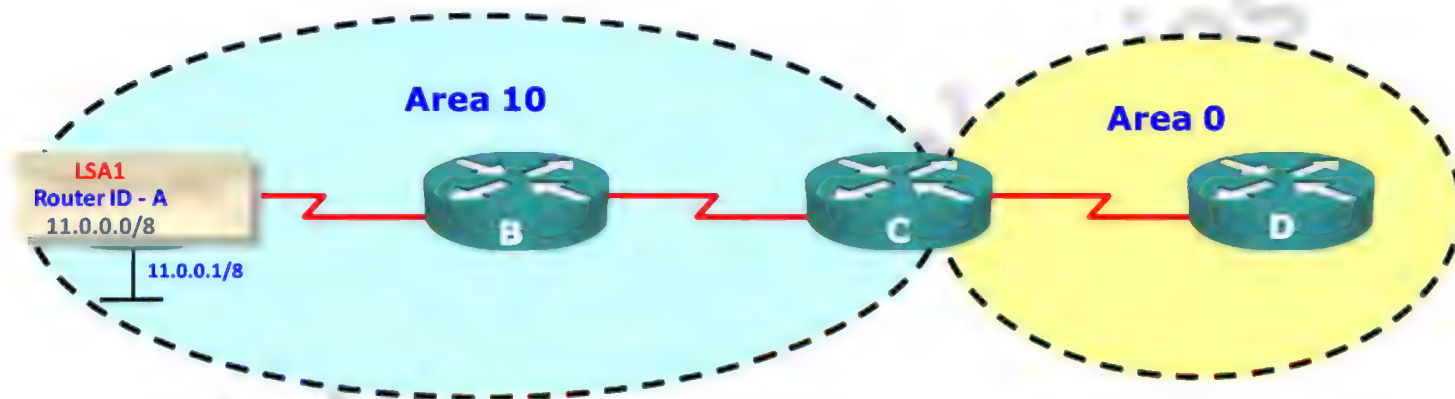
LS Types	Name
1	Router LSAs
2	Network LSAs
3	Summary LSAs
4	ASBR Summary
5	Autonomous System External LSAs
6	Multicast OSPF LSA
7	Defined for not-so-stubby areas

LSA Type 1: Router LSA

- One Router LSA (type 1) for every router in an area
 - Includes list of directly attached links
 - Each link identified by IP prefix and link type
- Identified by the router ID of the originating router
- Floods within its area only; does not cross the ABR

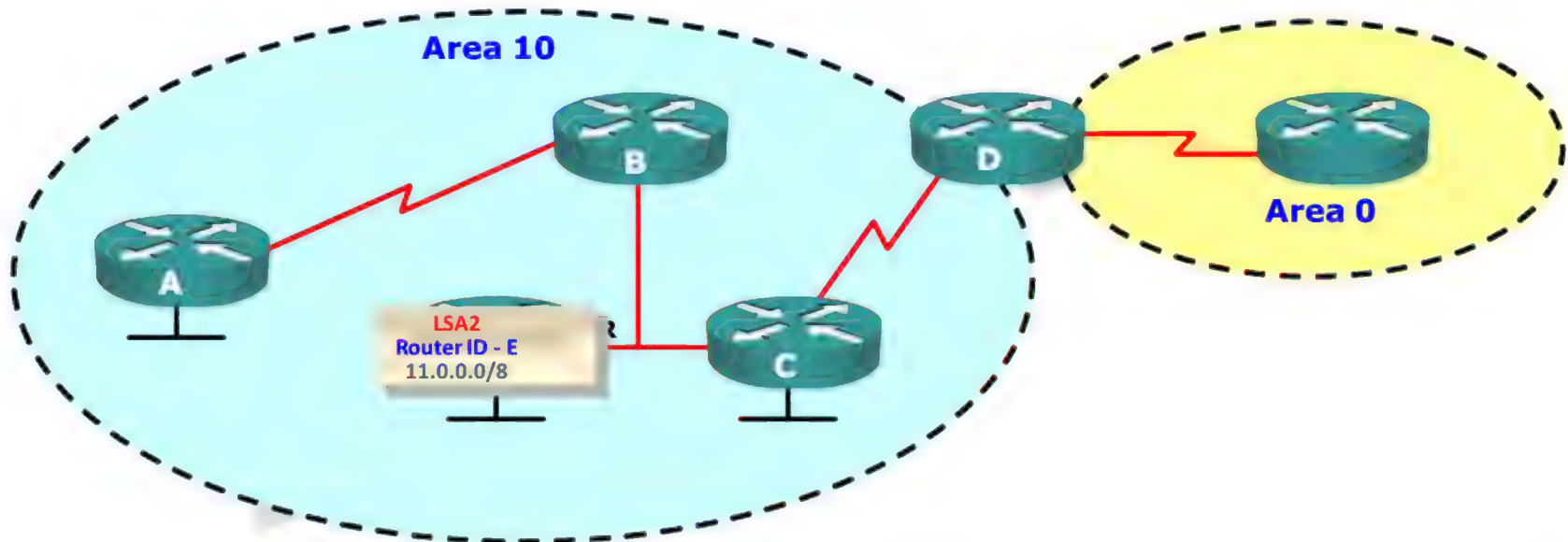
Zoom Technologies

LSA Type 1: Router LSA



LSA Type 2: Network LSA

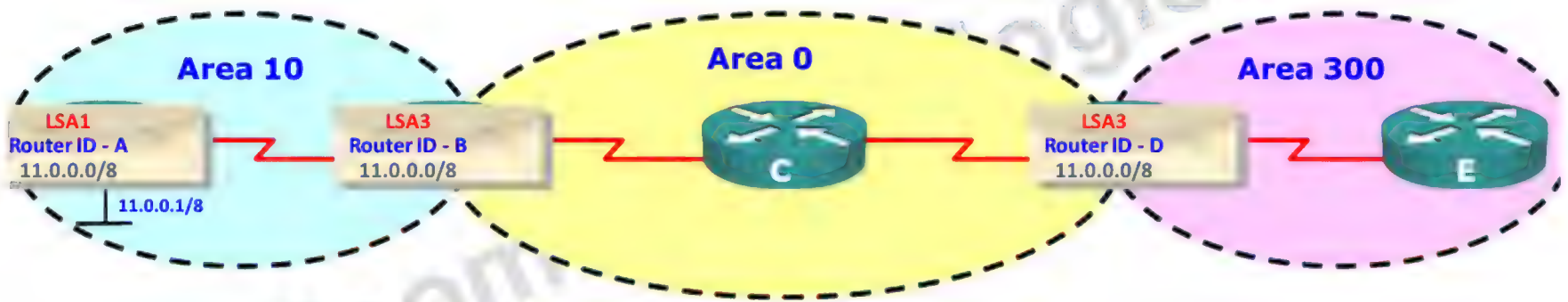
- One Network (type 2) LSA for each transit broadcast or NBMA network in an area
 - Includes Network ID, subnet mask and list of attached routers on that transit link
- Advertised by the DR of the transit network
- Floods within its area only; does not cross ABR



- Type 3 LSAs are used to flood network information to areas outside the originating area (inter-area)
 - contains network ID and subnet mask
- Advertised by the ABR of originating area
- Regenerated by subsequent ABRs to flood throughout the autonomous system.
- By default, routes are not summarized and there is one type 3 LSA for every subnet

Zoom Technologies

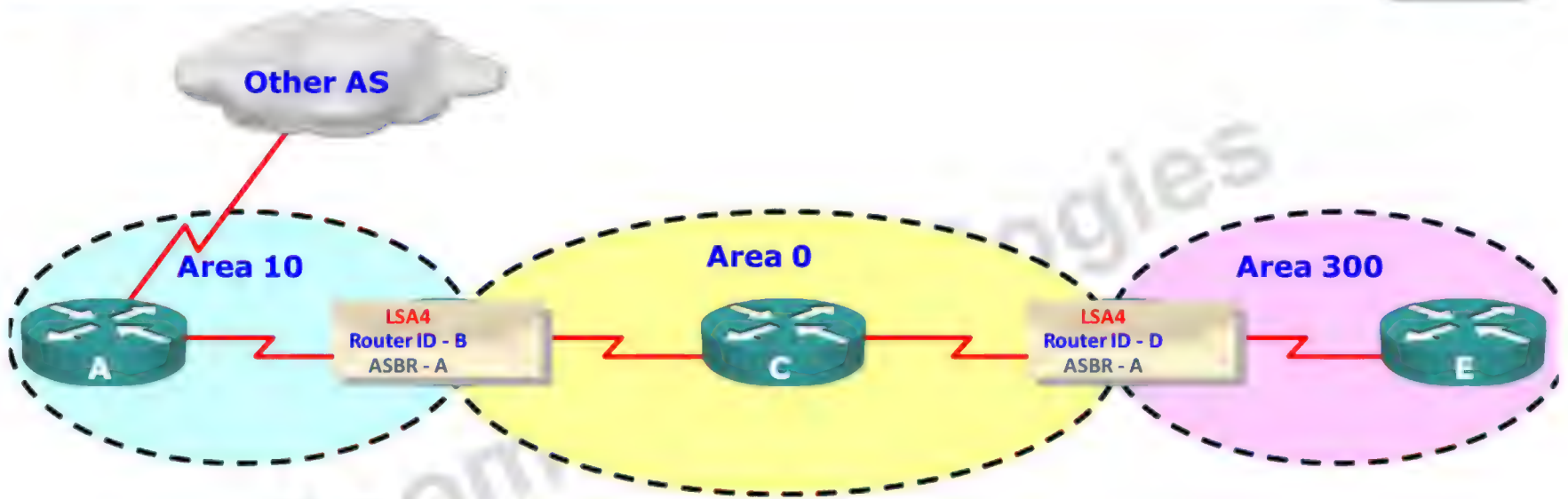
LSA Type 3: Summary LSA



LSA Type 4: ASBR Summary LSA

- ASBR Summary (type 4) LSAs are used to advertise Router ID of ASBR to all routers in other areas present in autonomous system
- They are generated by the ABR of the originating area
- They are regenerated by all subsequent ABRs to flood throughout the autonomous system
- Type 4 LSAs contain only the router ID of the ASBR

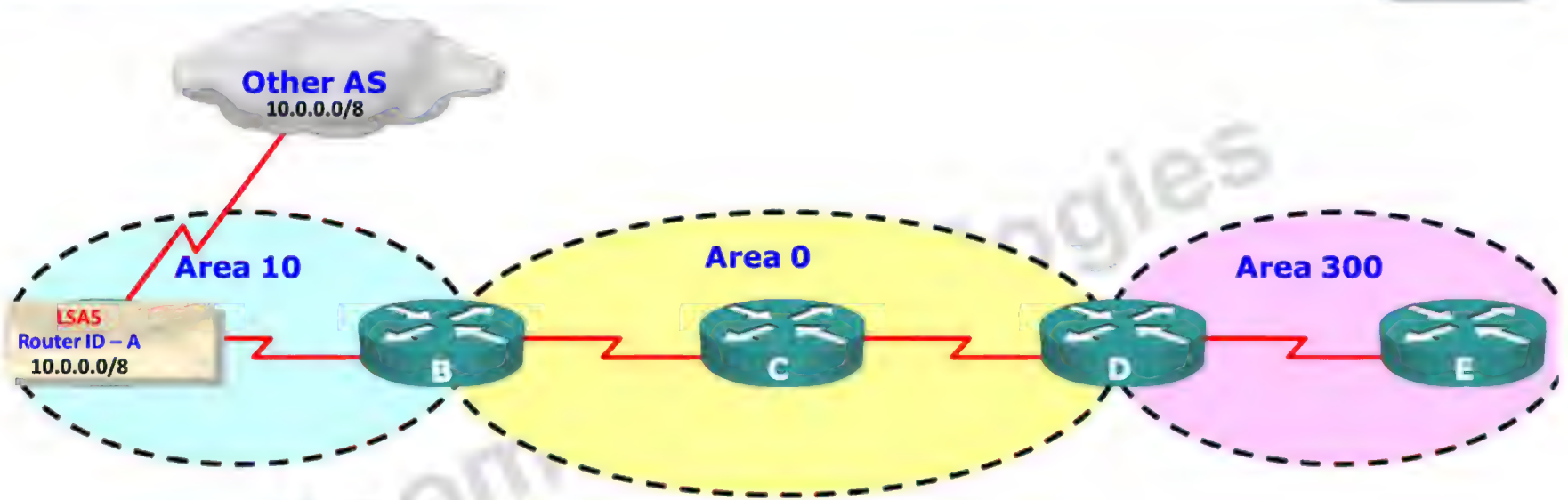
LSA Type 4: Summary LSA



LSA Type 5: External LSA

- External (type 5) LSAs are used to advertise networks learned from other autonomous systems
- Type 5 LSAs are advertised and owned by the originating ASBR
- Type 5 LSAs flood throughout the autonomous system
- The advertising router ID (ASBR) is unchanged throughout the autonomous system
- Type 4 LSA is needed to identify ASBR
- By default, routes are not summarized by ASBR

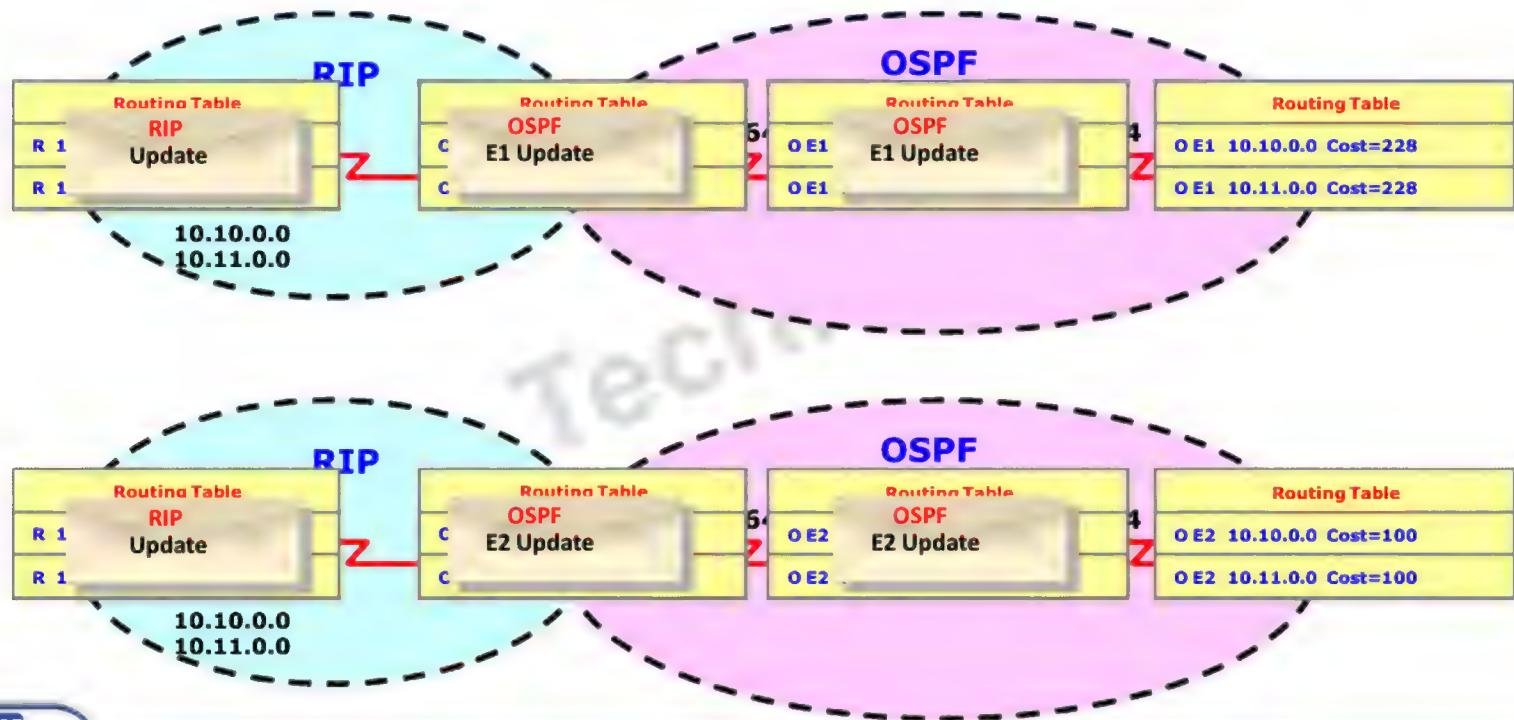
LSA Type 5: External LSA



Types of Routes

Router Designator		Description
O	LSA 1	Networks from within the area of the router
O IA	OSPF interarea (summary LSA)	Networks from outside the area of the router, but within the OSPF autonomous system
O E1	E1 external routes	Networks outside of the autonomous system of the router
O E2	E2 external routes	

Cost for External Updates

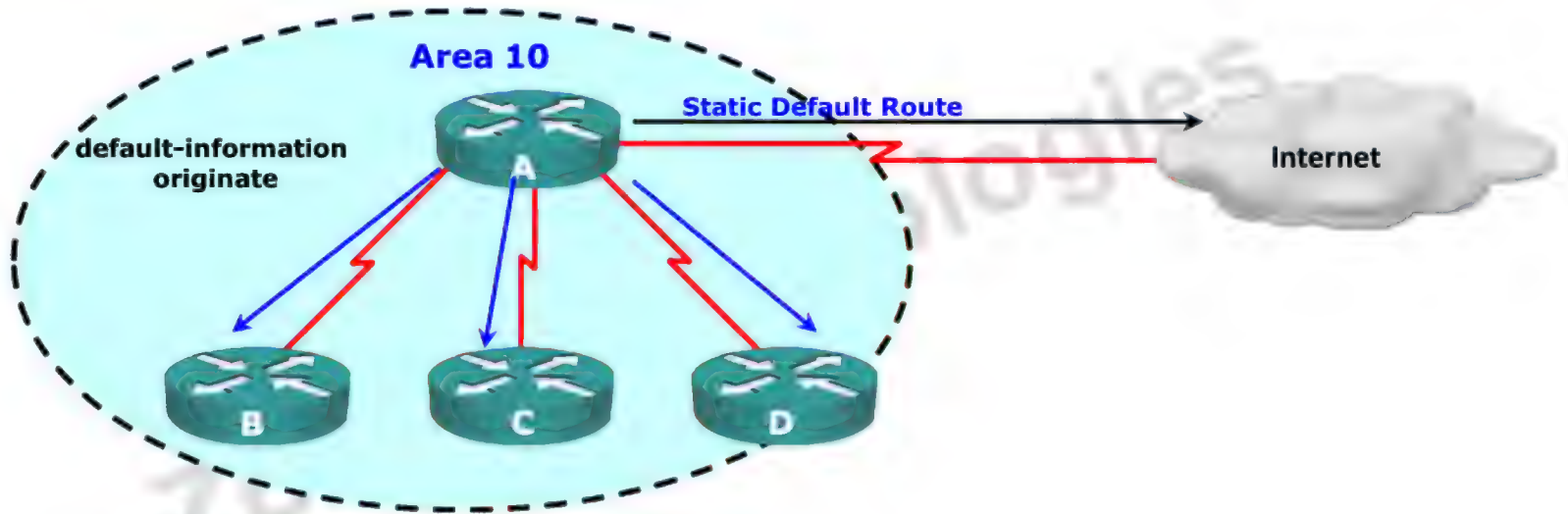


Default Routes in OSPF

- OSPF can send Default Route in update
- A default route is sent as an external LSA type (O*E2)
- Static Default Route needs to be defined in Originating router

Router(config)# **ip route 0.0.0.0 0.0.0.0 <Exit Int/next-hop-IP>**

Router(config-router)# **default-information originate**



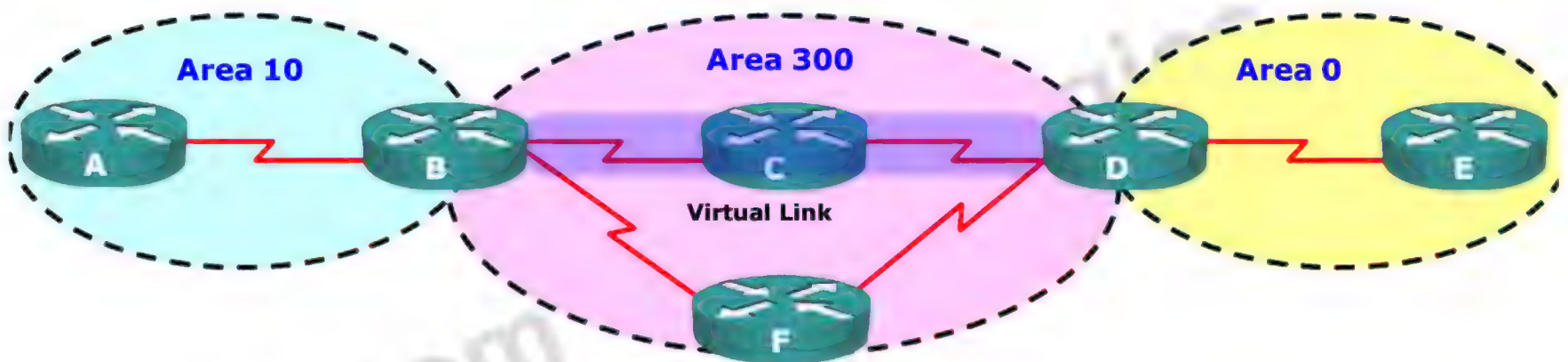
OSPF Virtual Link

Defining Virtual Links

- Virtual links are used to connect a discontinuous area to area 0
- A logical connection is built between routers
- Virtual links are recommended for backup or temporary connections

Zoom Technologies

Virtual Links



Zoom

Configuring Virtual Link

```
Router(config-router)# area <area-id> virtual-link  
                        <router-id>
```

Zoom Technologies



OSPF Special Area



Stub and Totally Stubby Area Rules



- There should not be an ASBR in the area
- The area should not be Area 0
- No virtual links must pass through the area
- There should be a single ABR (recommended)

Zoom Technologies



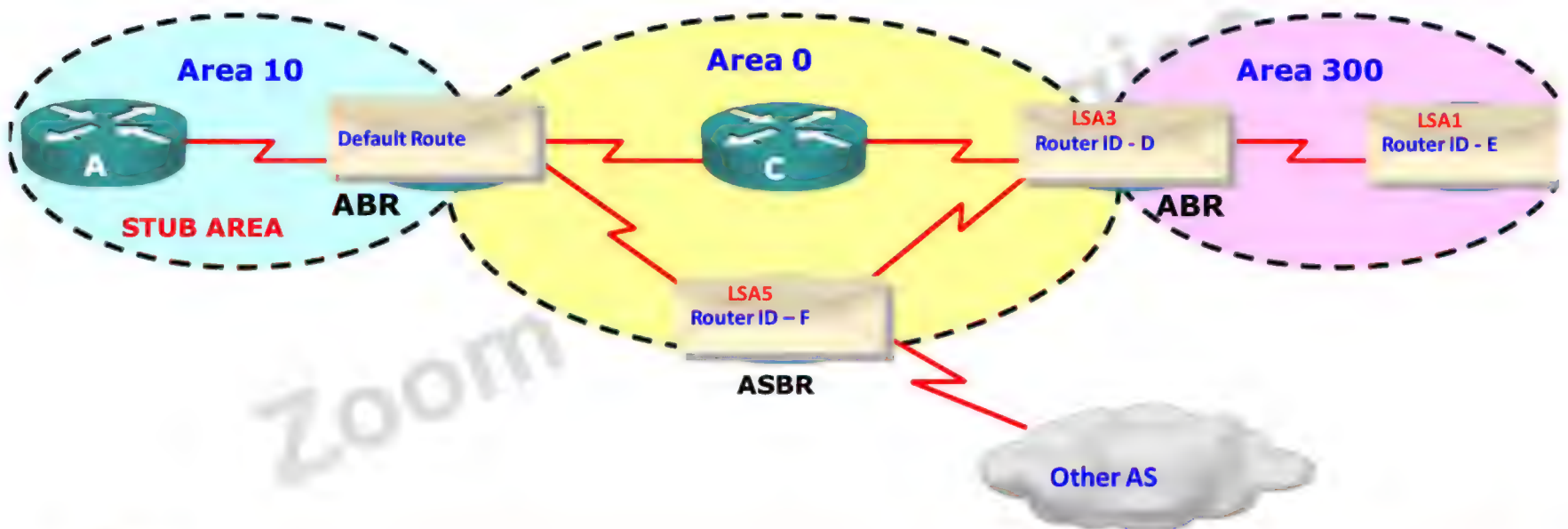
Using Stub Areas



- External LSAs are stopped
- Default route is advertised into stub area by the ABR
- All routers in stub area must be configured as stub

Zoom Technologies





Configuring Stub command on all router in the area

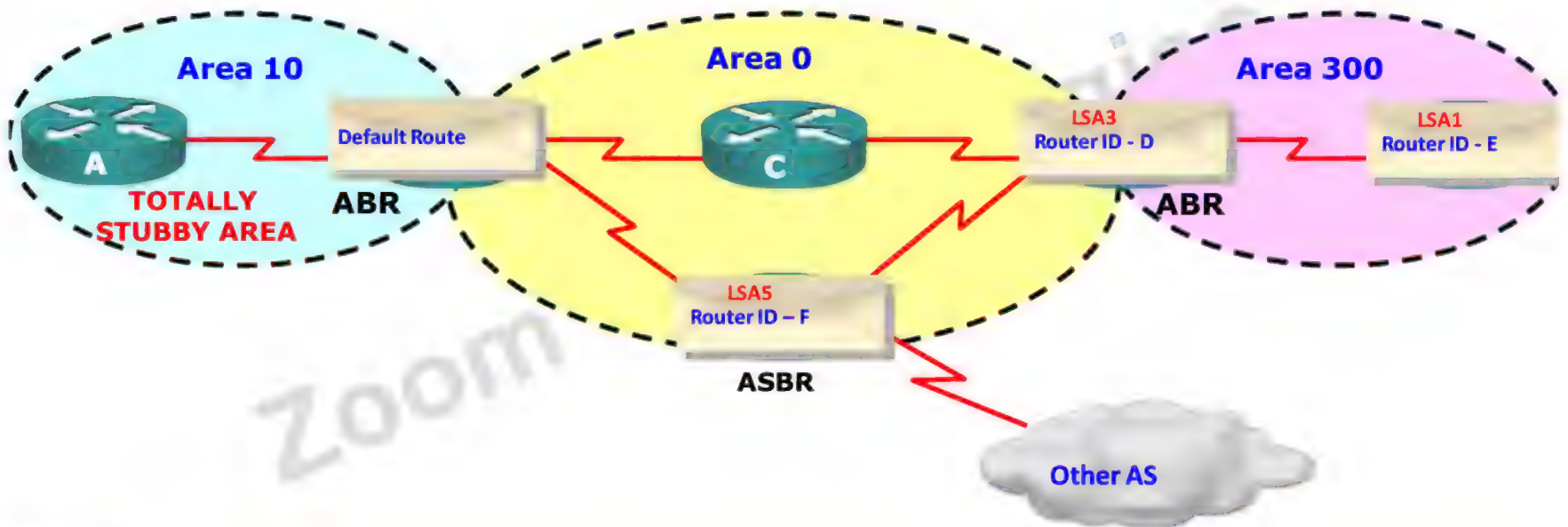
```
Router(config-router)# area <area-id> stub
```

Using Totally Stubby Areas

- External LSAs are stopped
- Summary LSAs are stopped
- Routing table is reduced to a minimum
- All routers in stub area must be configured as stub
- ABR of stub area must be configured as totally stubby
- This is a Cisco proprietary feature

Zoom Technologies

Totally Stubby Area



Totally Stubby Configuration



Configuring all routers of Totally Stubby Area

```
Router(config-router)# area <area-id> stub
```

Configuring Area Border Router of Totally Stubby Area

```
Router(config-router)# area <area-id> stub no-summary
```

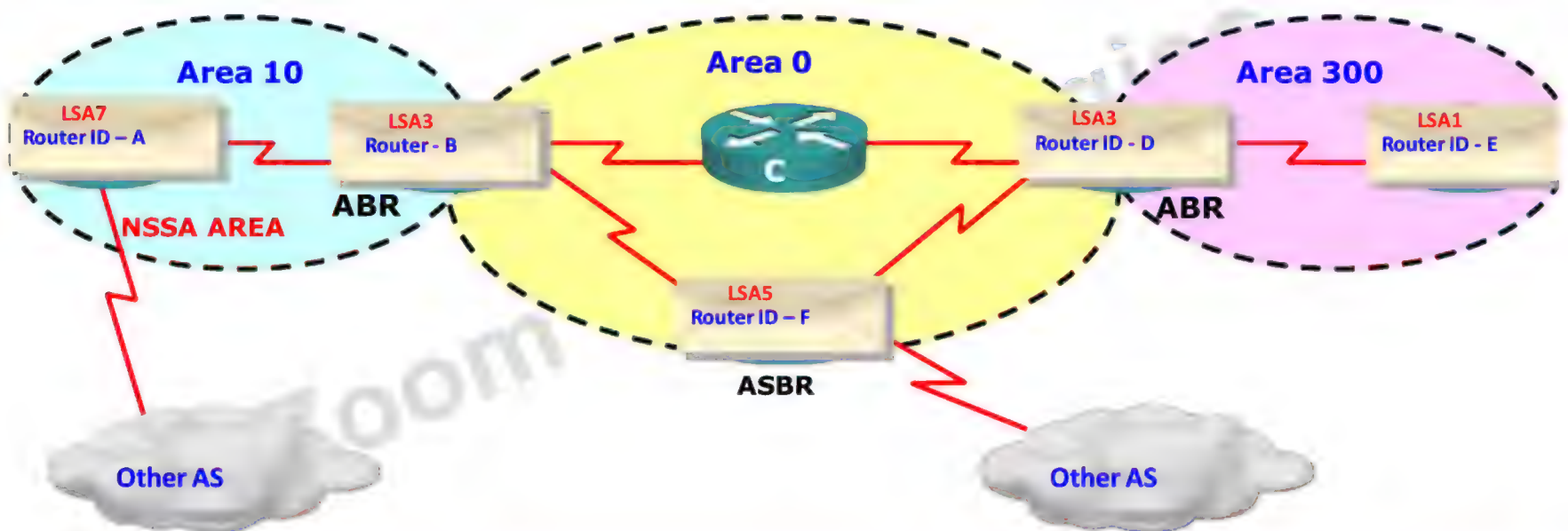


Not-So-Stubby Areas



- NSSA breaks stub area rules
- ASBR is allowed in NSSA
- Special LSA type 7 defined, sent by ASBR
- ABR converts LSA type 7 to LSA type 5
- ABR does not send default route into NSSA by default
- NSSA is an RFC addendum





Configuring NSSA command on all router in the area

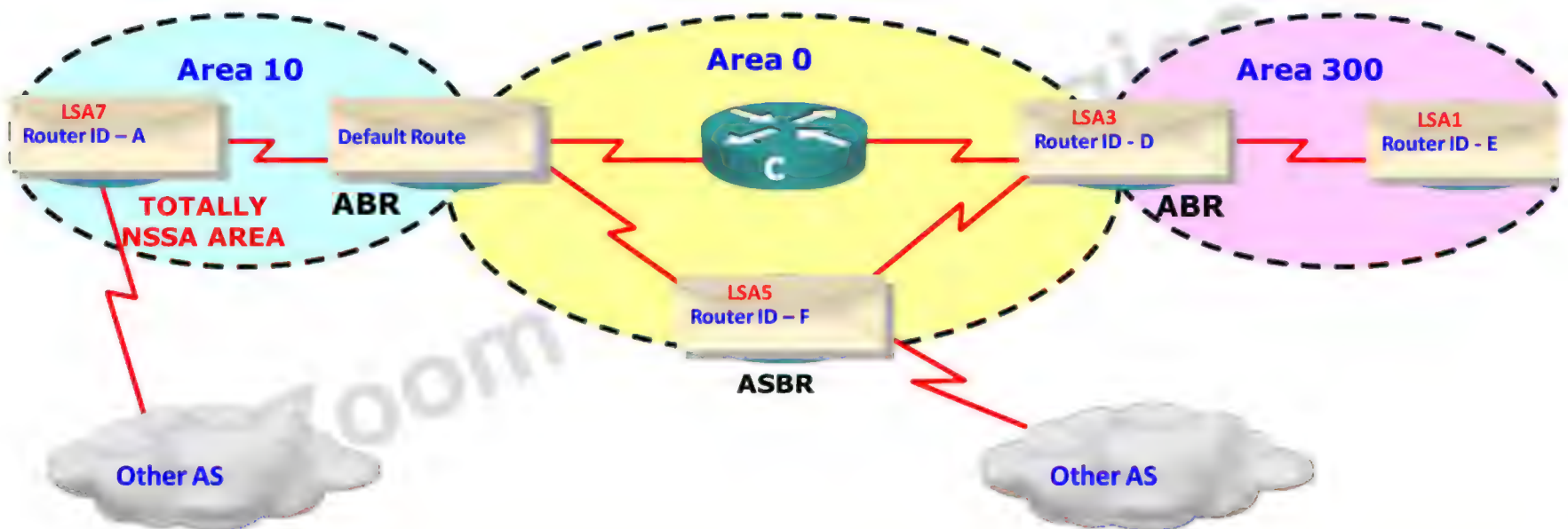
```
Router(config-router)# area <area-id> nssa
```

Totally Not-So-Stubby Areas

- Totally NSSA Does not accept summary and external LSAs
- By default, Default Route is advertised by ABR of Totally NSSA

Zoom Technologies

Totally NSSA Area



Totally NSSA Area Configuration



Configuring NSSA command on all routers in the area

```
Router(config-router)# area <area-id> nssa
```

Configuring NSSA command on ABR router in the area

```
Router(config-router)# area <area-id> nssa no-summary
```



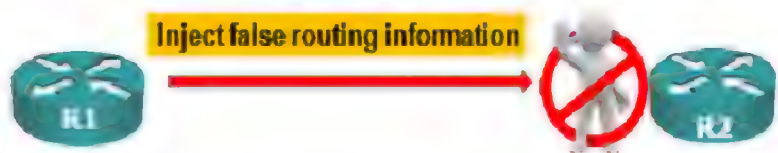
OSPF Authentication



OSPF supports two types of routing protocol authentication methods

1) Clear Text or Plain Text

2) MD-5 Authentication



Routers will accept the routing information from other routers that have been configured with the same password or authentication information.



1) Clear Text or Plain Text

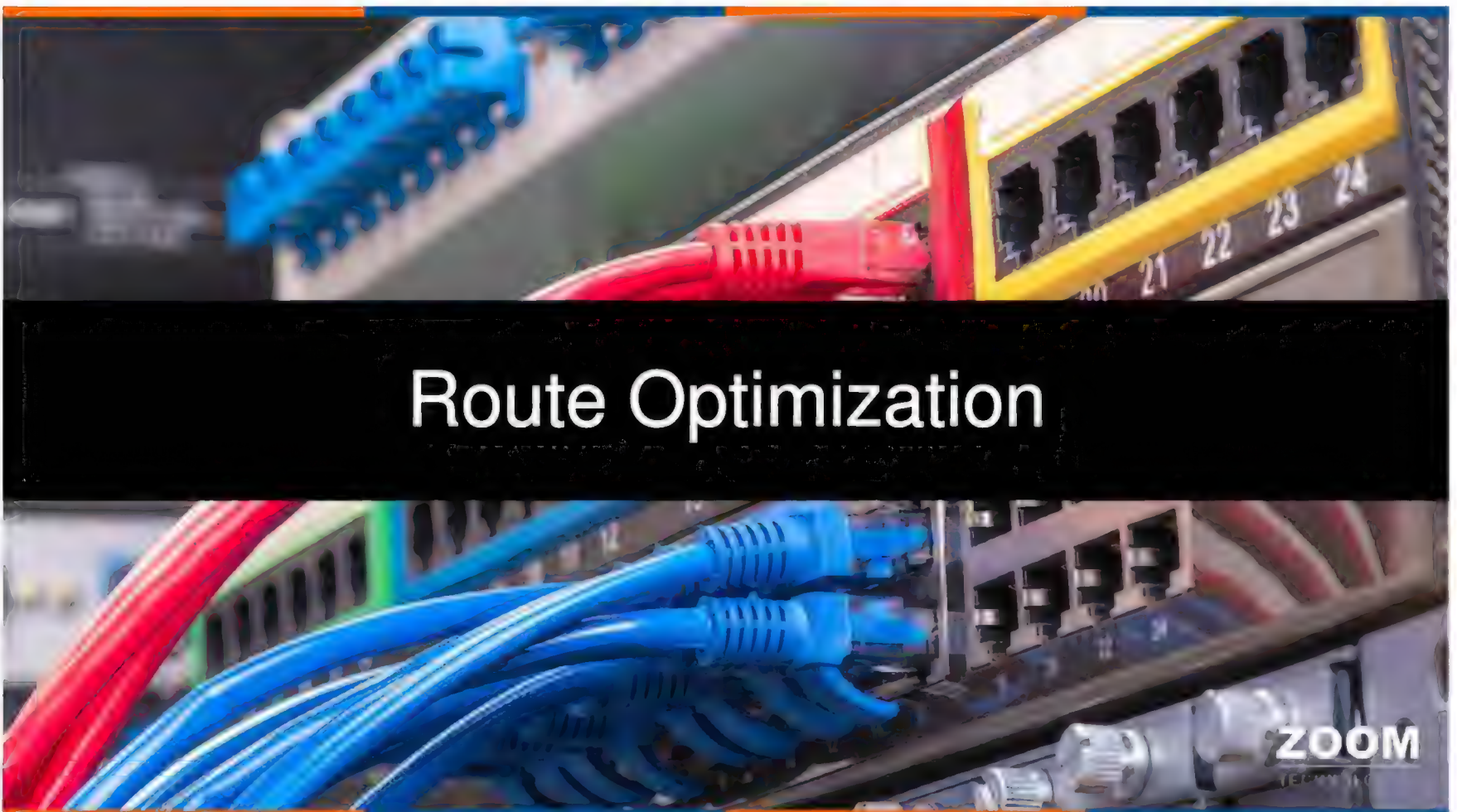
```
Router(conf-if)#ip ospf authentication
```

```
Router(conf-if)# ip ospf authentication-key ccnp
```

2) MD-5 Authentication

```
Router(conf-if)#ip ospf authentication message-digest
```

```
Router(conf-if)# ip ospf message-digest-key key-id md5 ccnp
```



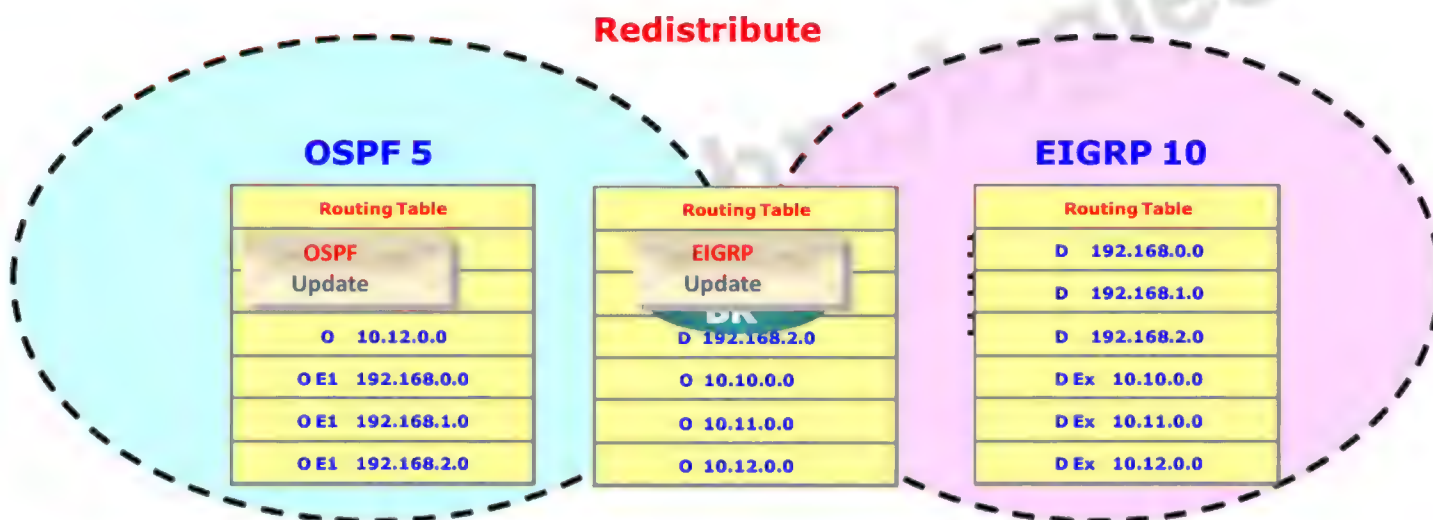
Reasons for using Multiple Routing protocols

- Application-specific protocols
- Mismatch between devices (Vendors)
- Political boundaries

Zoom Technologies

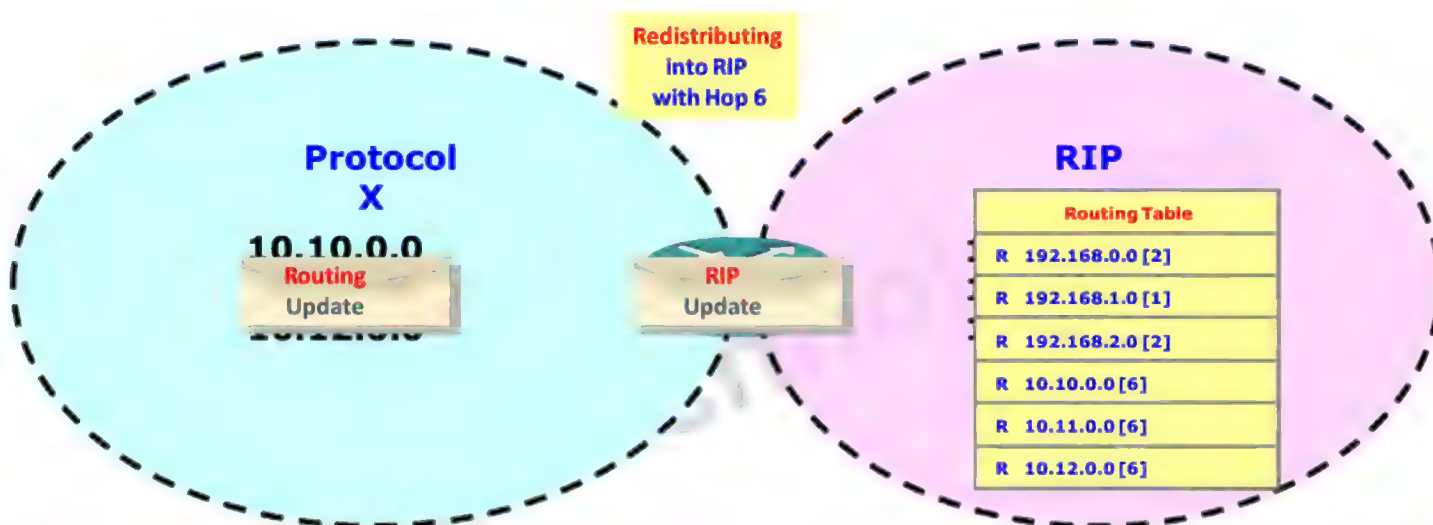
Redistribution

- This process of exchanging routing information between routing protocols is called **Route Redistribution**



Protocols	Metric
RIP	Infinite
OSPF	20
IGRP and EIGRP	Infinite
IS - IS	0
BGP	From IGP

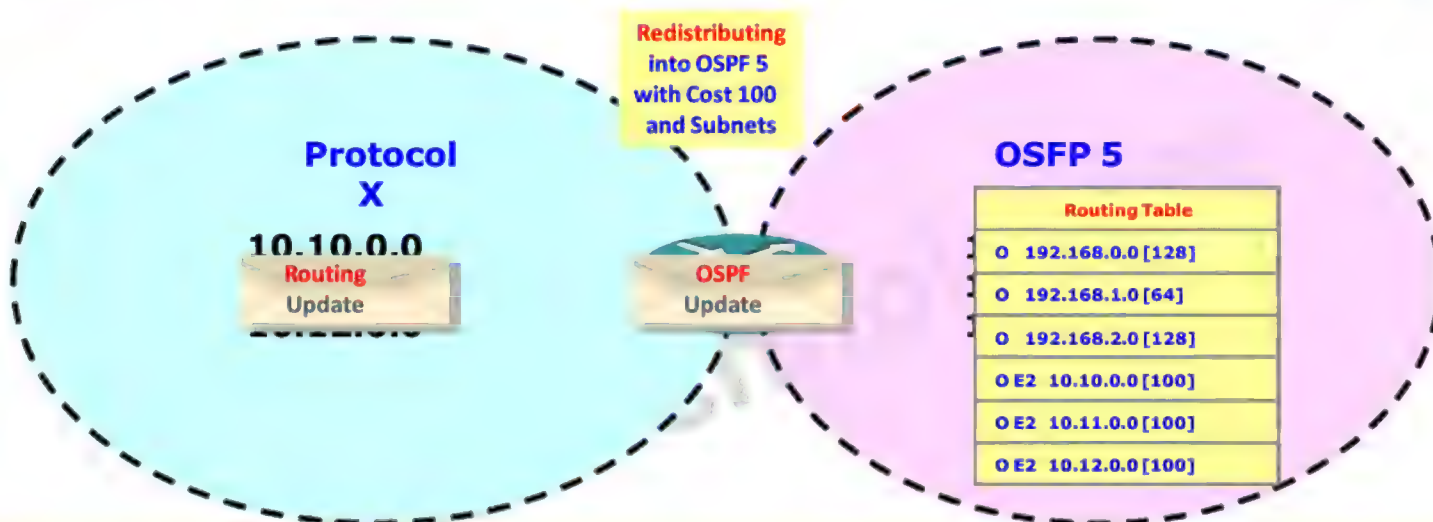
Redistributing into RIP



Configuring Redistribution into RIP

```
BR(config)# router rip
BR(config-router)# redistribute <protocol>
metric <value>
```

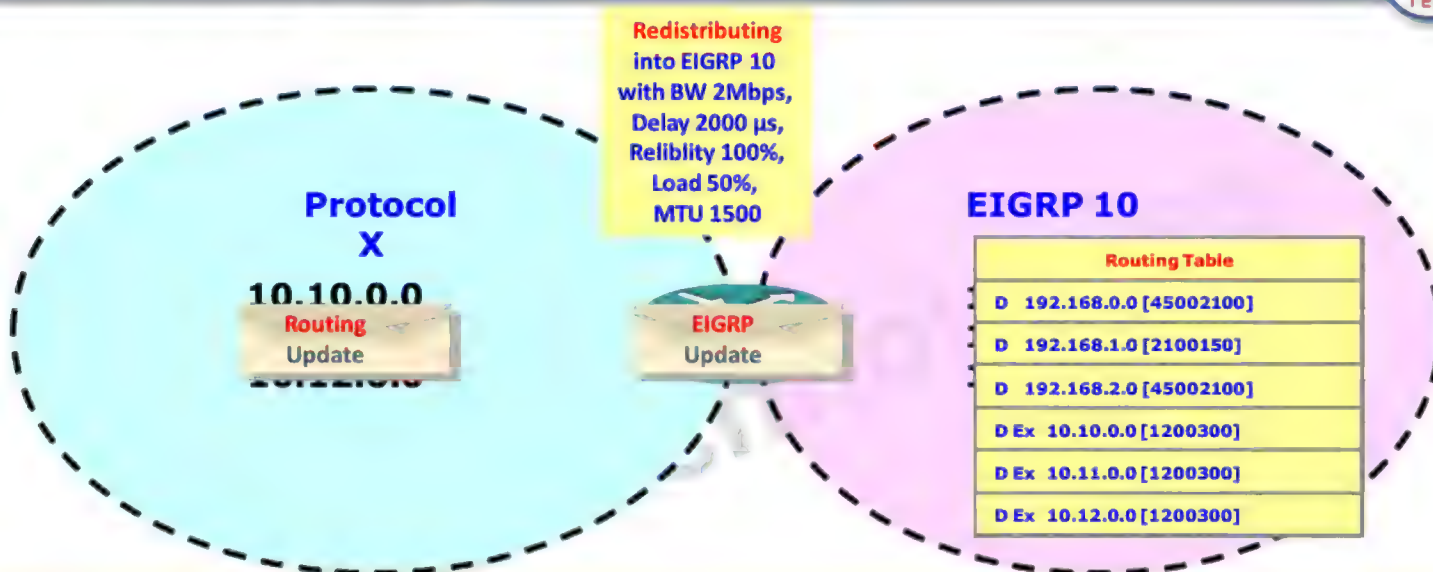
Redistributing into OSPF



Configuring Redistribution into OSPF

```
BR(config)# router ospf 5
BR(config-router)# redistribute <protocol>
                        [metric <value>] [metric-type 1|2]
                        [subnet]
```

Redistributing into EIGRP

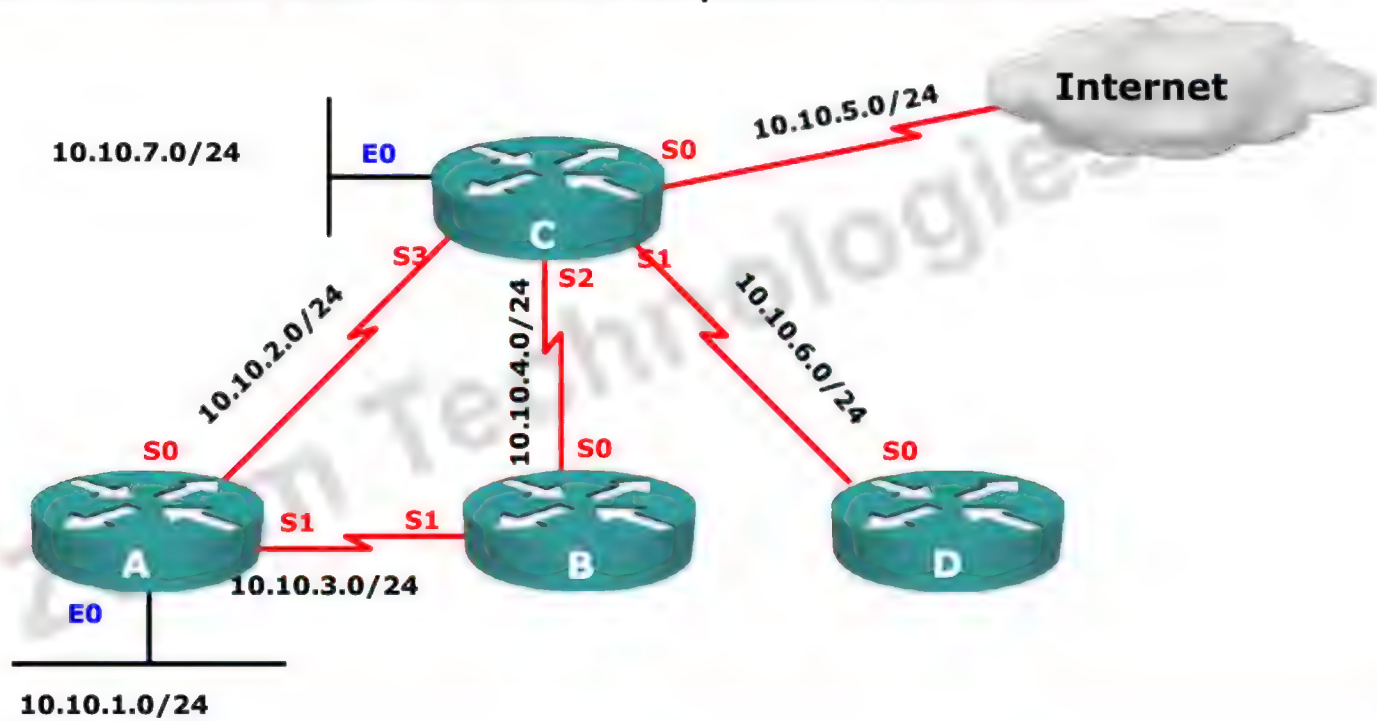


Configuring Redistribution into EIGRP

```
BR(config)# router eigrp 10
BR(config-router)# redistribute <protocol>
                        metric <BW in Kbps> <delay in µs>
                        <reliability> <load> <MTU>
```

Passive Interface

Passive Interface is the interface which will not send hello packets on the interface

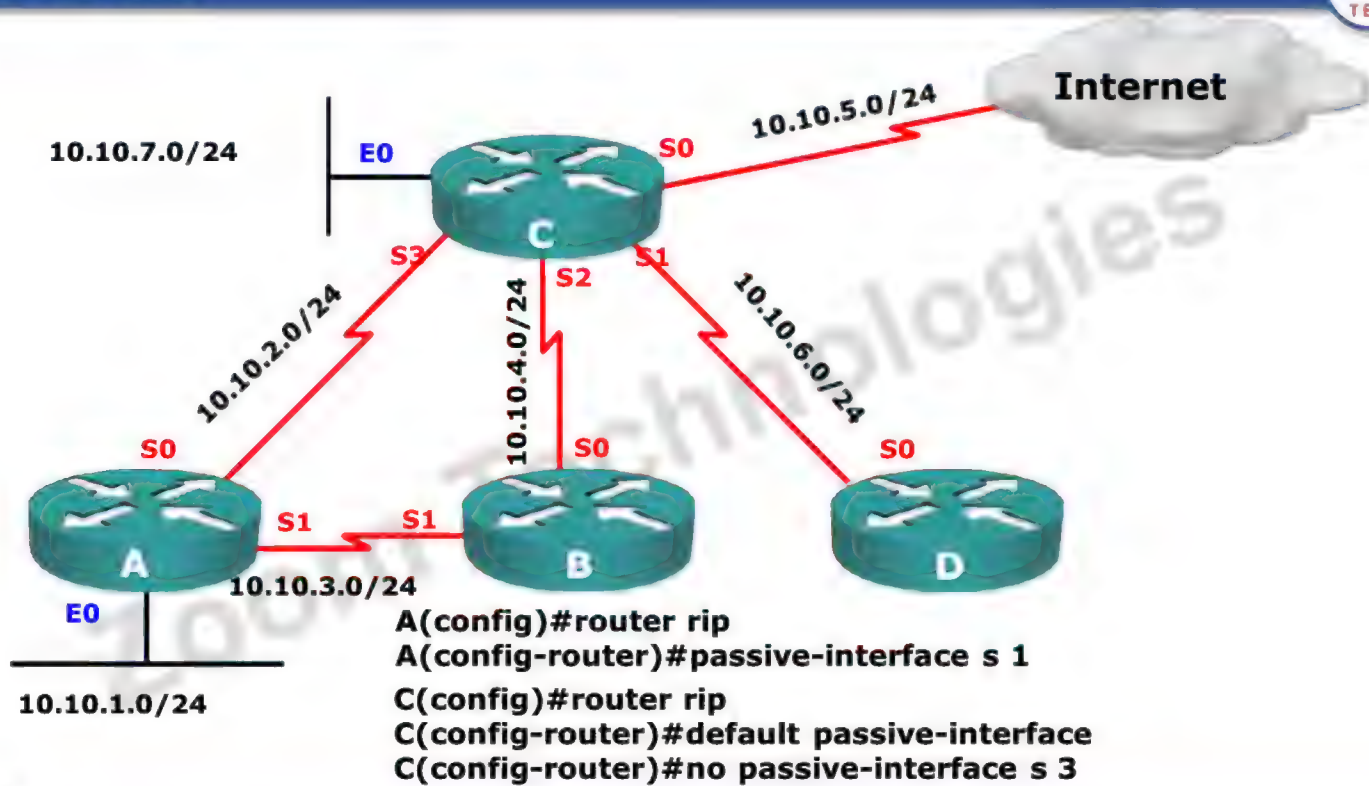


Passive Interface Command

Configuring Passive Interface in routing protocol

Router(config-router)# **passive-interface** <type> <No.>

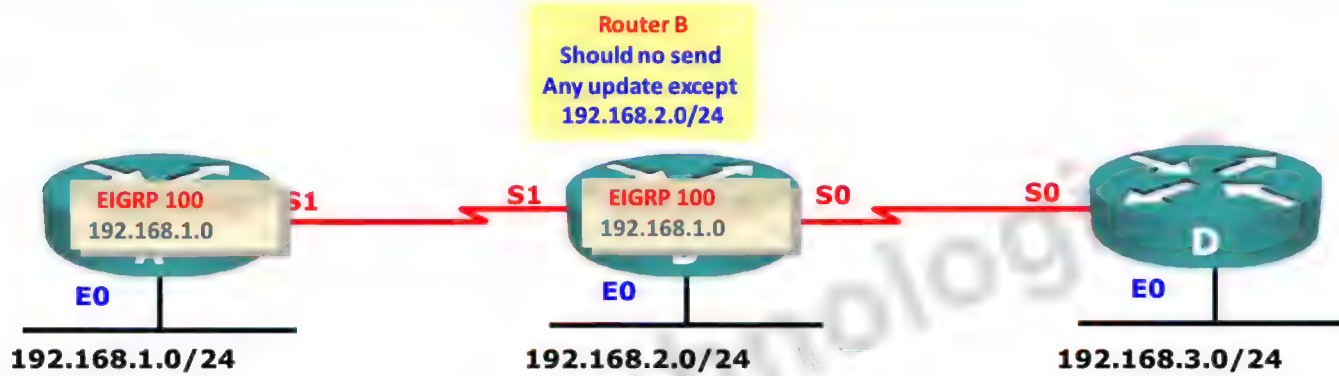
Passive Interface



Distribute Lists

- Distribute List is a method of filtering routing updates.
- Filtering can be inbound or outbound.
- Distribute List will be applied in router mode.

Distribute List

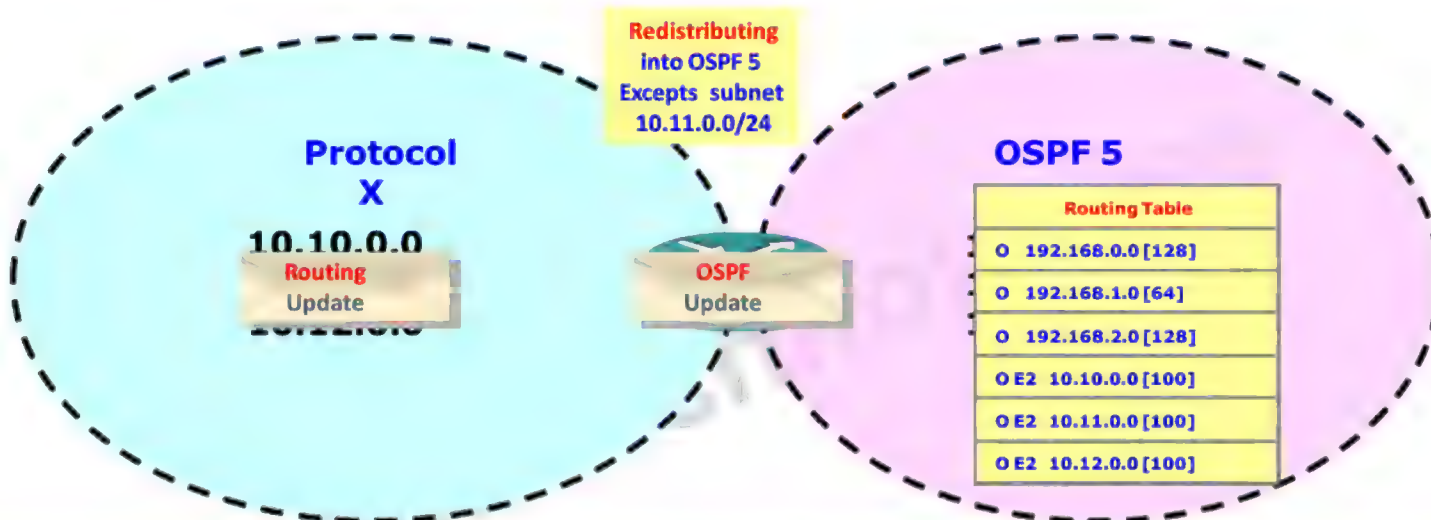


Configuring Distribute-list on Router B

Router(config)# **Router eigrp 100**

Router(config-router)# **distribute-list <ACL-No.> <in / out >**
<int type> <No.>

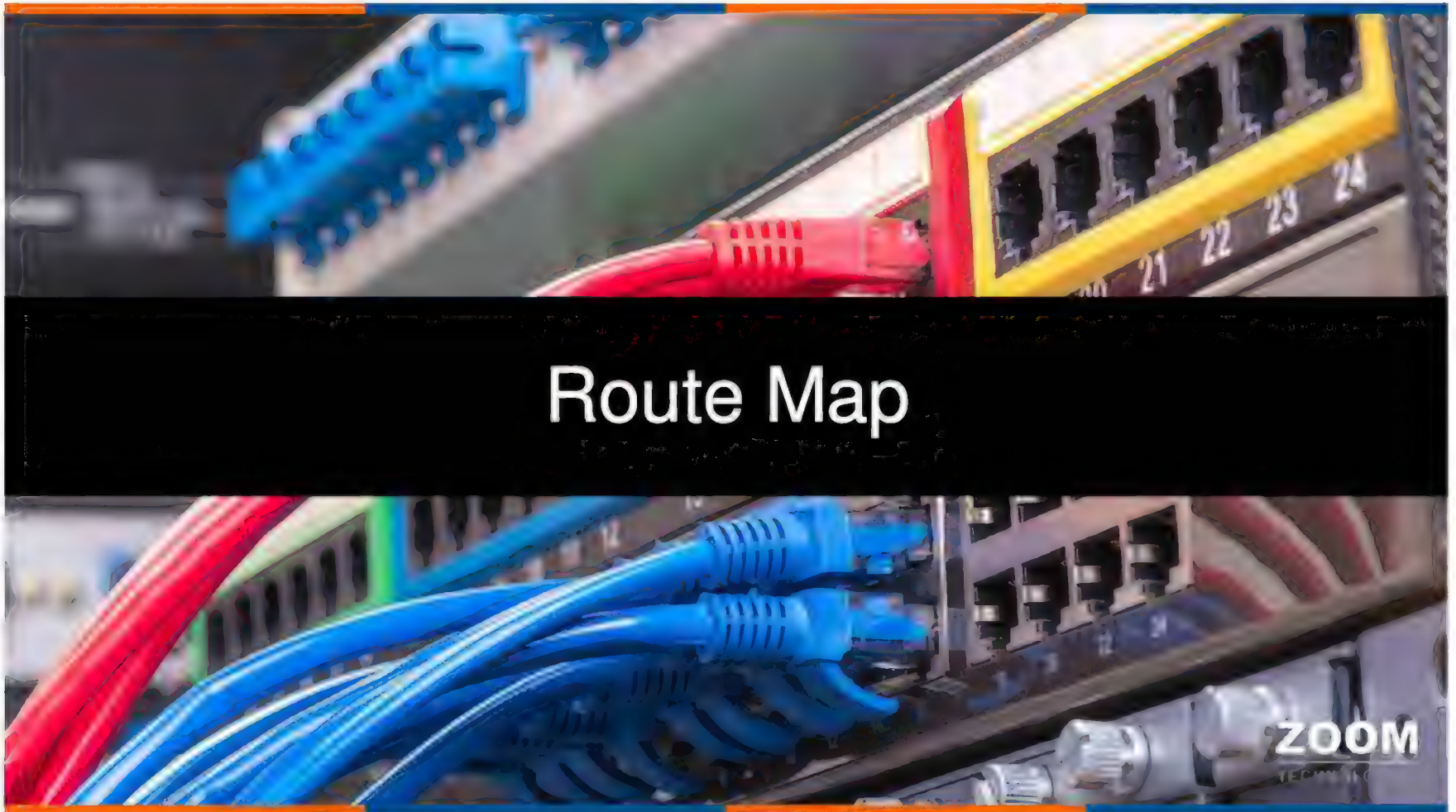
Distribute List



Configuring Distribute-list on Router B

Router(config)# **Router ospf 5**

Router(config-router)# **distribute-list <ACL-No.> out**
<protocol>



ROUTE Maps

ZOOM
TECHNOLOGIES

- Route maps work like a scripting language
- It works like a sophisticated access-list
- Top down processing
- Once a match is found , the remaining statements are no longer processed
- Route maps are configured with sequence numbers for easy editing i.e. for adding ,removing and inserting new statements.
- Route maps are identified by names
- Route maps will follow "IF THEN ELSE" criteria



ROUTE MAPS – Usage

- Route maps are used for
 - policy based routing
 - BGP policy
 - Redistribution
 - NAT
 - QoS

Zoom Technologies

Configuration Of Route MAP

Configure Route Map

Router(config)# **Route-map** <name> **permit/deny** <Sequence No.>

Defining the condition to Match

Router(config-route-map)#**match** <condition>

Defining the condition to Set

Router(config-route-map)#**set** <condition>



Policy Based Routing

POLICY BASED Routing

ZOOM
TECHNOLOGIES

- It is used for implementing a policy that causes the packet to take a different direction
- Routing table is destination based
- PBR allows source based routing

Zoom Technologies



POLICY BASED Routing



- **ADVANTAGES**
- Different users can use different paths to reach the destination
- Load sharing

Zoom Technologies



POLICY BASED Routing



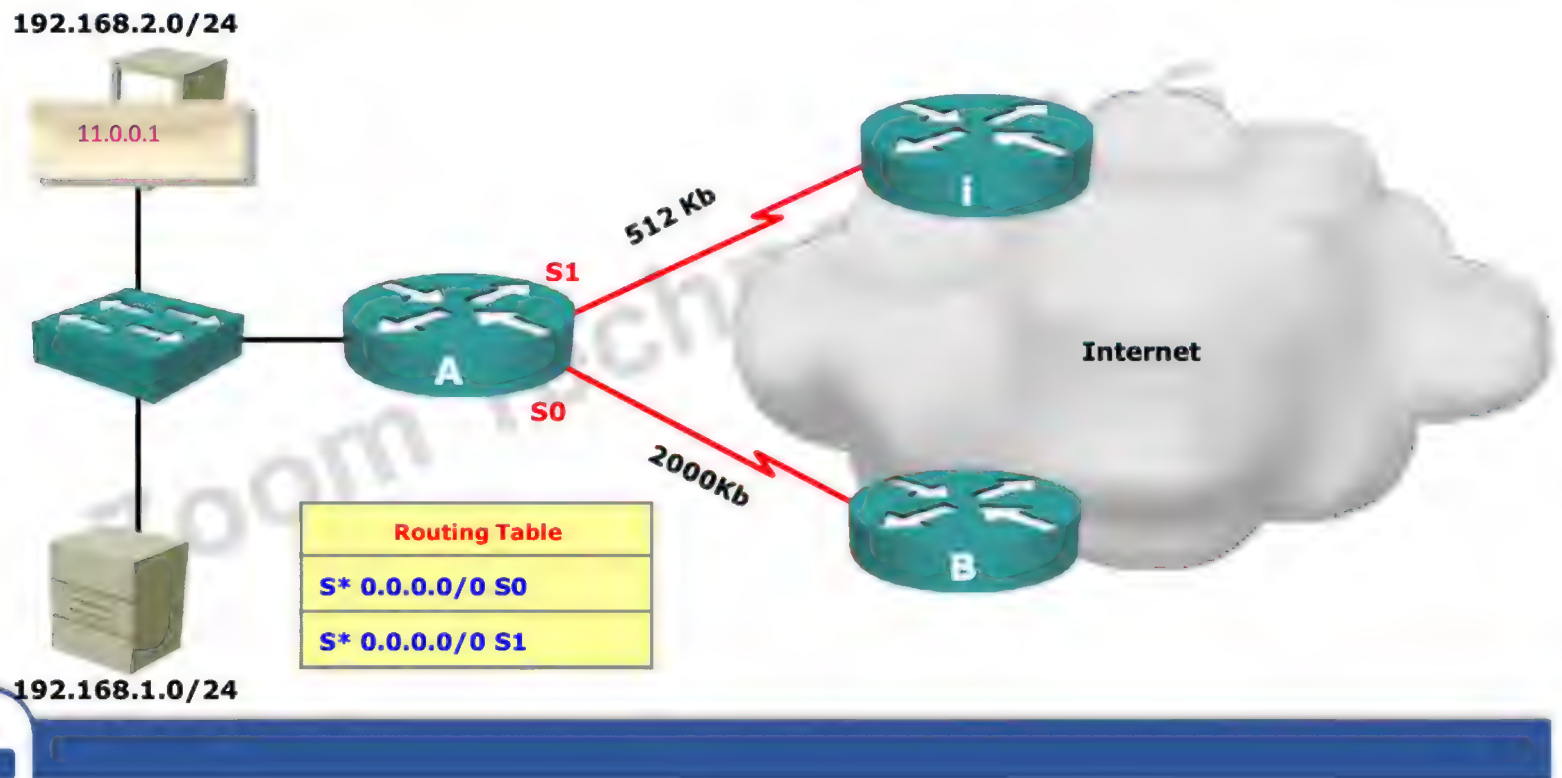
Features

- Implemented in the incoming direction of the source interface
- If a match is found in the route map and it is permitted , the packet will be sent according to the policy
- If a match is found in the route map and it's not permitted , then it will be forwarded according to the normal routing table.
- If there is no match th Route-map the packet will be forwarded according to routing table

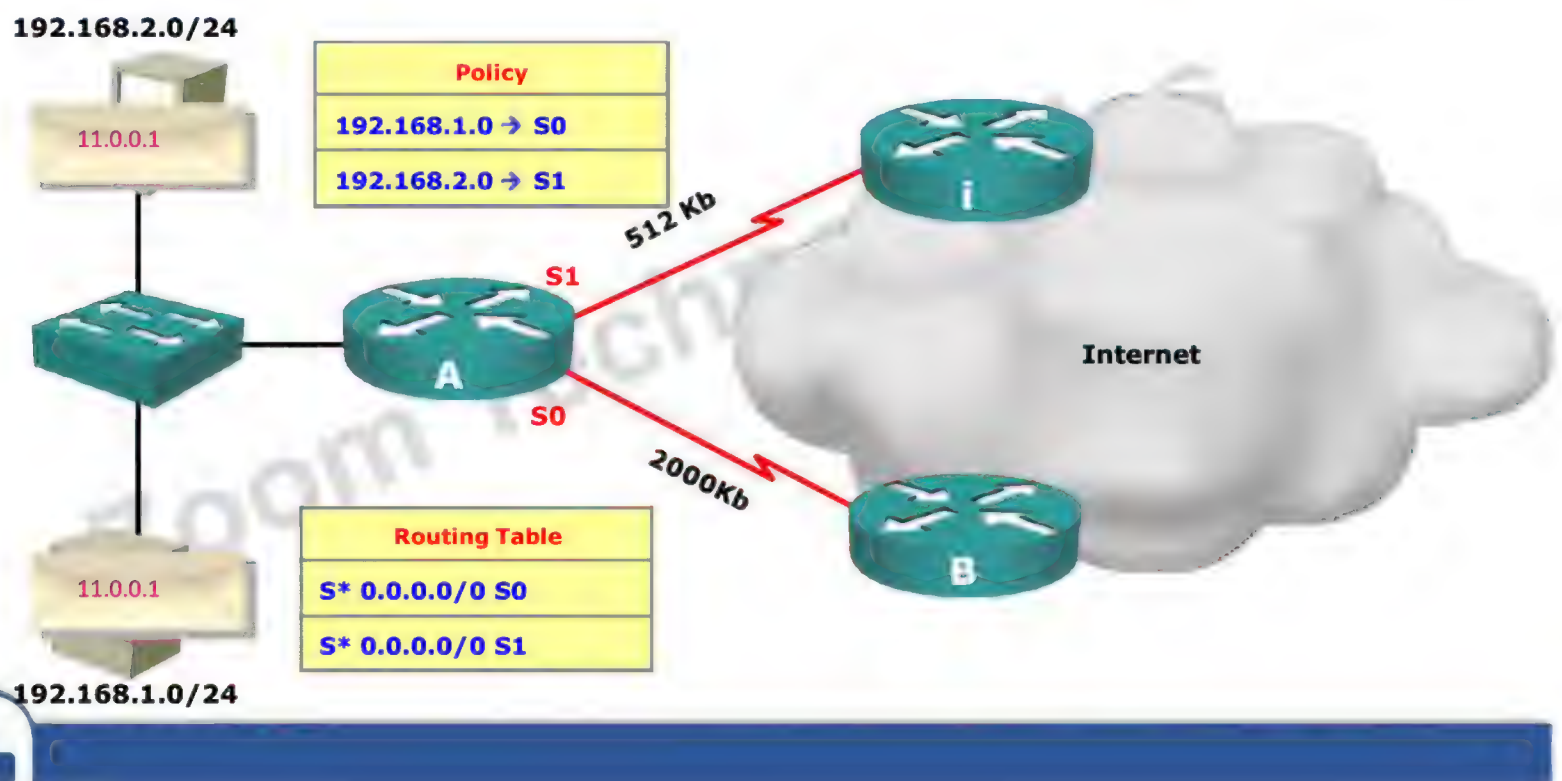
Zoom Technologies



Before POLICY BASED ROUTING



POLICY BASED Routing



Configure Route Map

```
Router(config)# Route-map <name> permit/deny <Sequence No.>
```

Defining the condition to Match

```
Router(config-route-map)#match ip address <ACL-No.>
```

Or

```
Router(config-route-map)#match interface <type> <No.>
```

Defining the condition to Set

```
Router(config-route-map)#set ip next-hop <next-hop IP>
```

Or

```
Router(config-route-map)#set interface <type> <No.>
```



Implementation Of PBR

```
Router(config-if)# ip policy route-map <name>
```



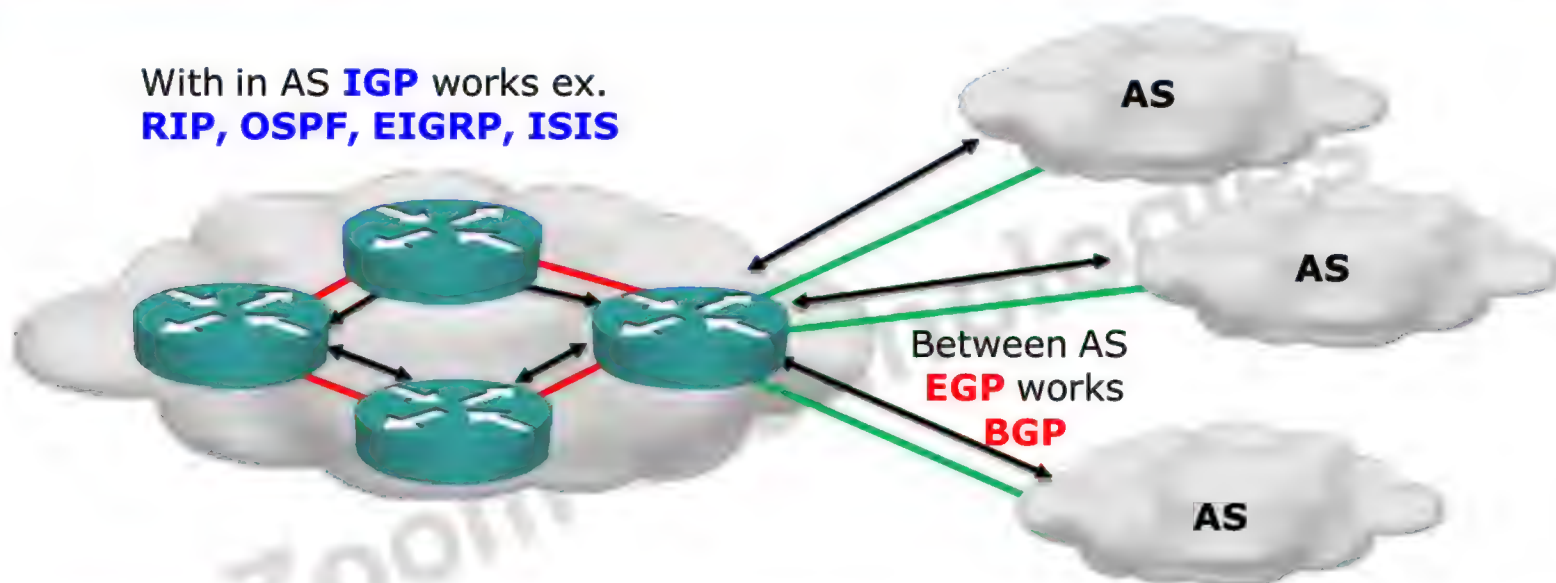
Border Gateway Protocol (BGP)



Autonomous System

ZOOM
TECHNOLOGIES

With in AS **IGP** works ex.
RIP, OSPF, EIGRP, ISIS



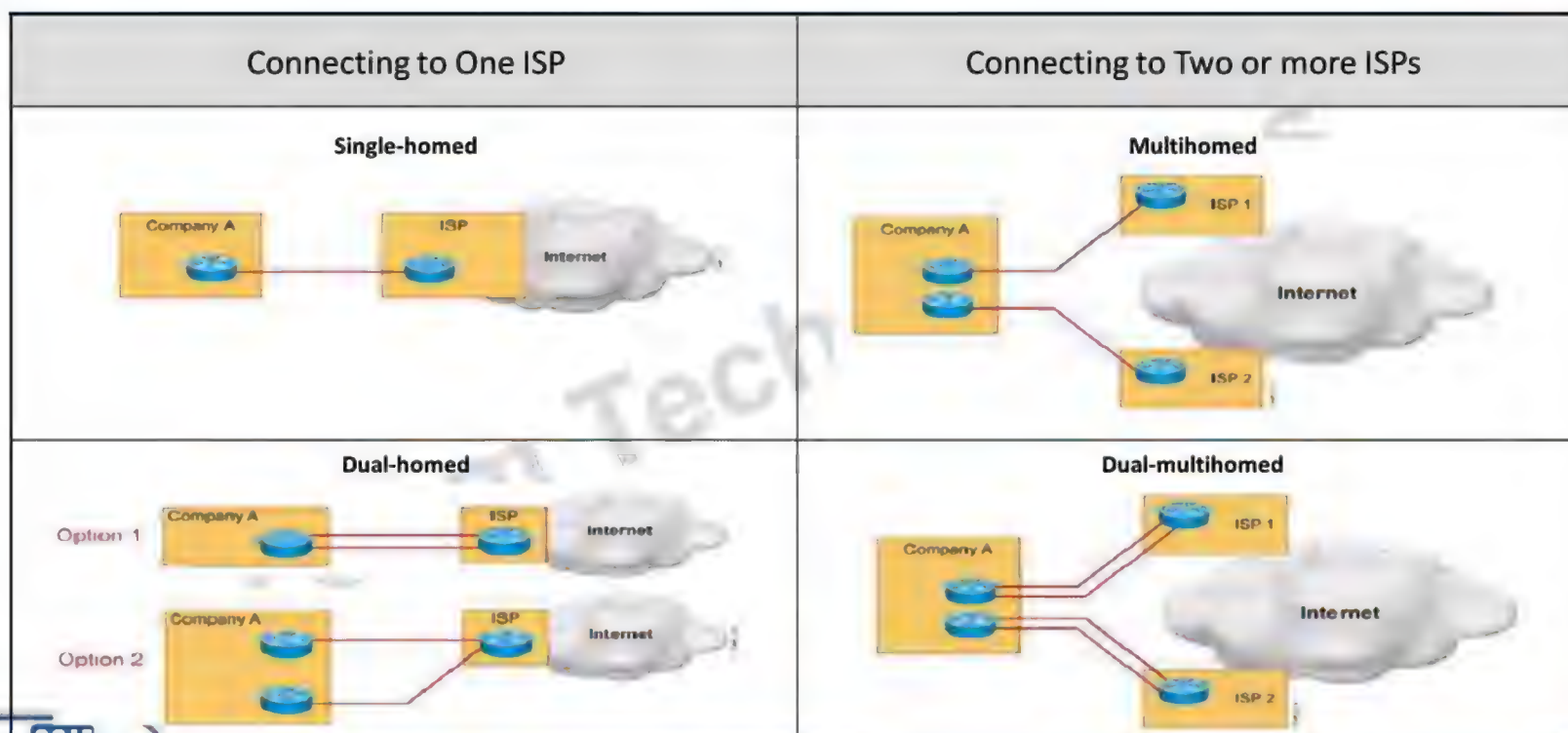
- **Autonomous System** is a set of routers under a single technical administration, using an interior gateway protocol and common metrics to route packets within the AS



The IANA is responsible for allocating AS numbers through five Regional Internet Registries (RIRs).



Connection Redundancy



When to use BGP

- BGP is more appropriate if one of the following conditions exist
 - A.S. Is working as transit A.S. (Ex. ISP)
 - A.S is connected to multiple A.Ss
 - The traffic path for data entering or leaving the A.S. needs to be manipulated

Zoom Technologies

When not to use BGP

- BGP is not recommended if one or more following conditions exist
 - If it is a Single-homed A.S
 - Lack of resources like memory and processing power in routers
 - Low bandwidth link between A.Ss
 - Limited understanding about BGP route filtering and path selection processes

Zoom Technologies

BGP Features

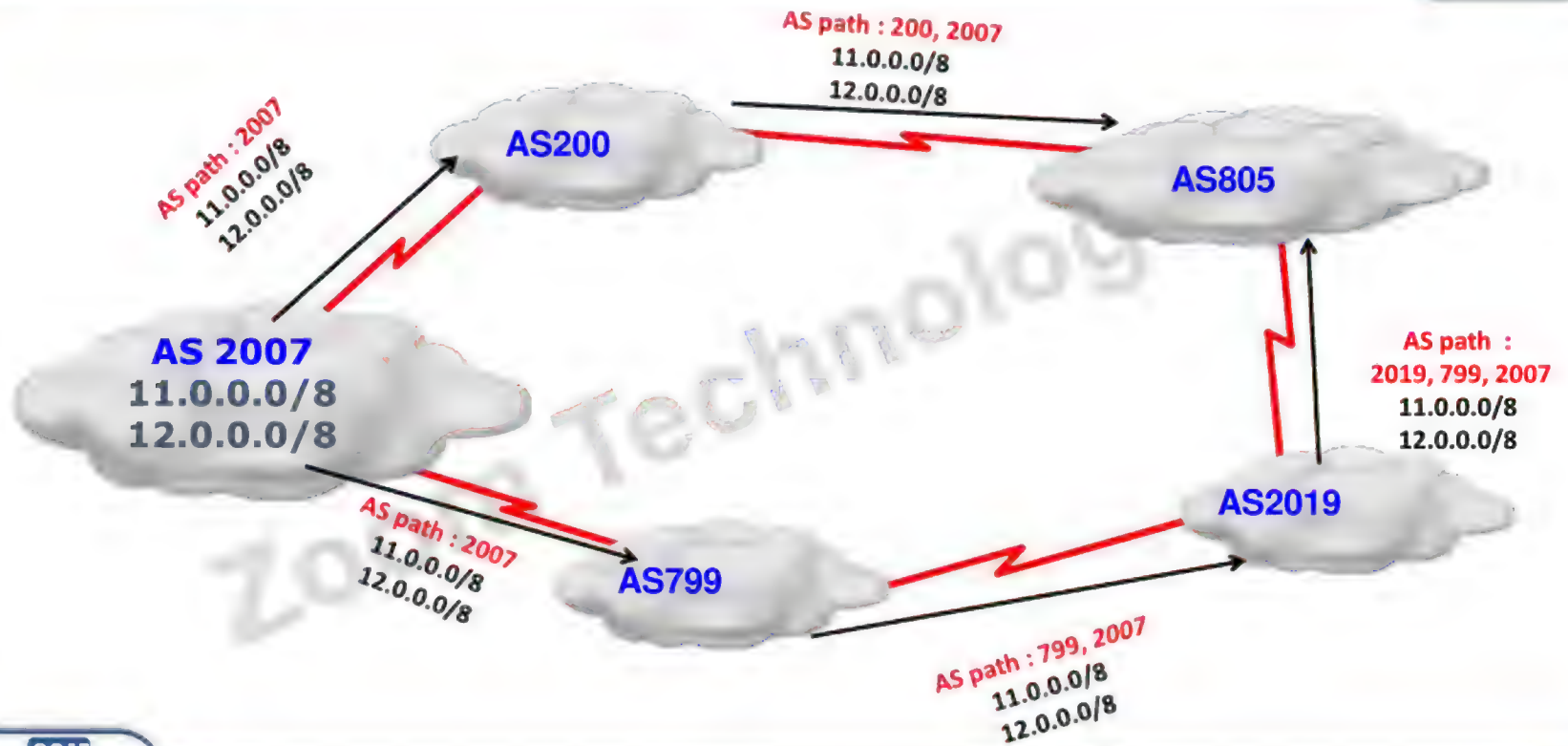
- Open Standard
- Advanced distance vector protocol
 - Path vector protocol
- Classless.
 - Support FLSM, VLSM, CIDR, auto and manual summary (BGP-4)
- It is an Exterior Gateway protocol
- Designed to scale up for a huge inter-network like the Internet.
- Updates are incremental and triggered.

BGP Features (continued)

- It sends updates to manually defined neighbors as unicast
- BGP is an application layer protocol, uses TCP for reliability, TCP port 179
- Metric = Attributes
- Administrative distance
 - 20 External updates
 - 200 Internal updates
- BGP is not designed for load balancing. Uses only one path per network

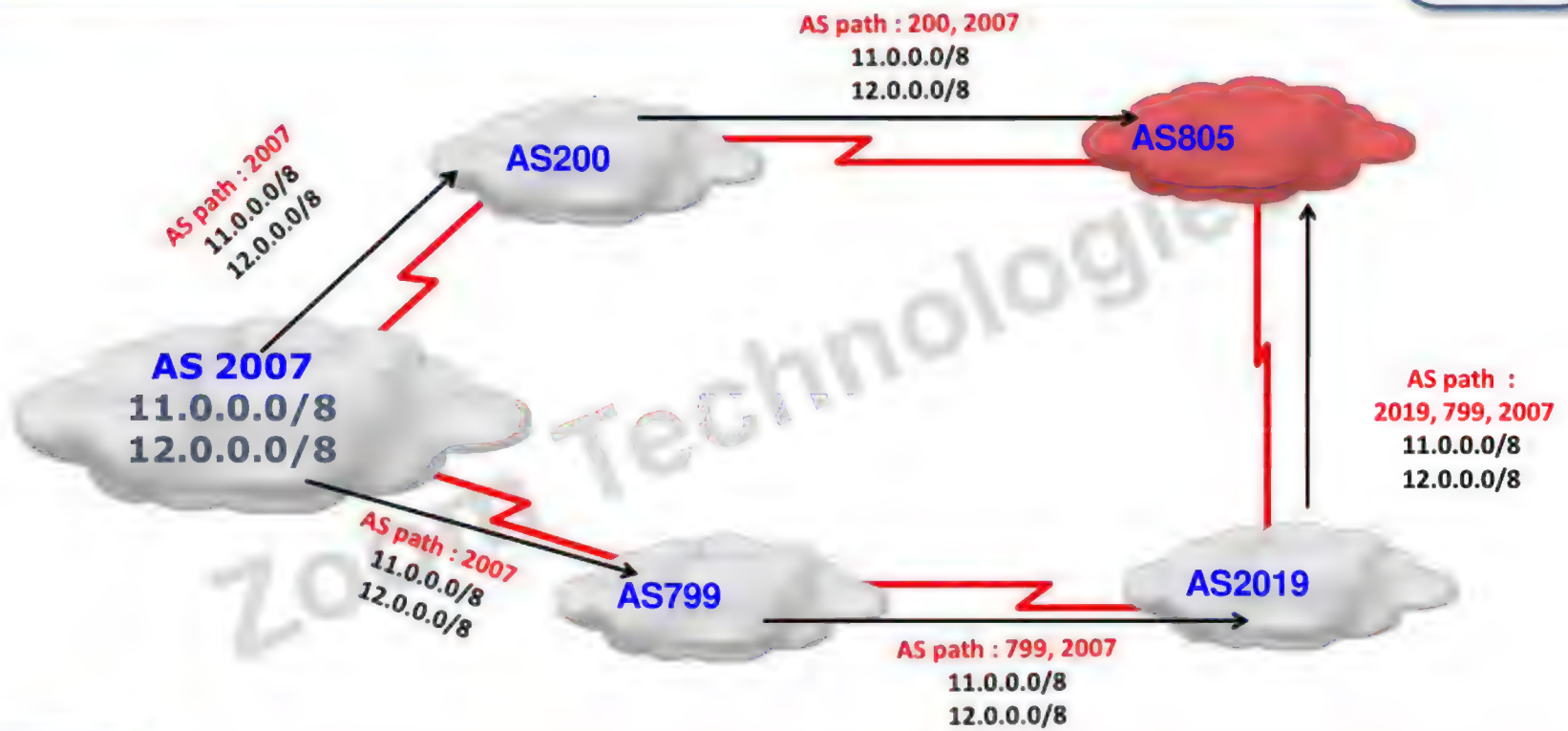
Path Vector

ZOOM
TECHNOLOGIES



Path Vector

ZOOM
TECHNOLOGIES



- IGP announce networks and cost to reach those networks.
- BGP announces pathways and the networks that are reachable at the end of the pathway. BGP uses Attribute as Metric.
- AS Path is one of the attribute of BGP. Path with less AS hop is best path.

- Neighbor table
 - List of BGP neighbours
- BGP forwarding table/database
 - List of all networks learned from each neighbor.
 - Can contain multiple pathways to destination networks
 - Database contains BGP attributes for each pathway
- IP routing table
 - List of best paths to destination networks

OPEN

Keep-Alive

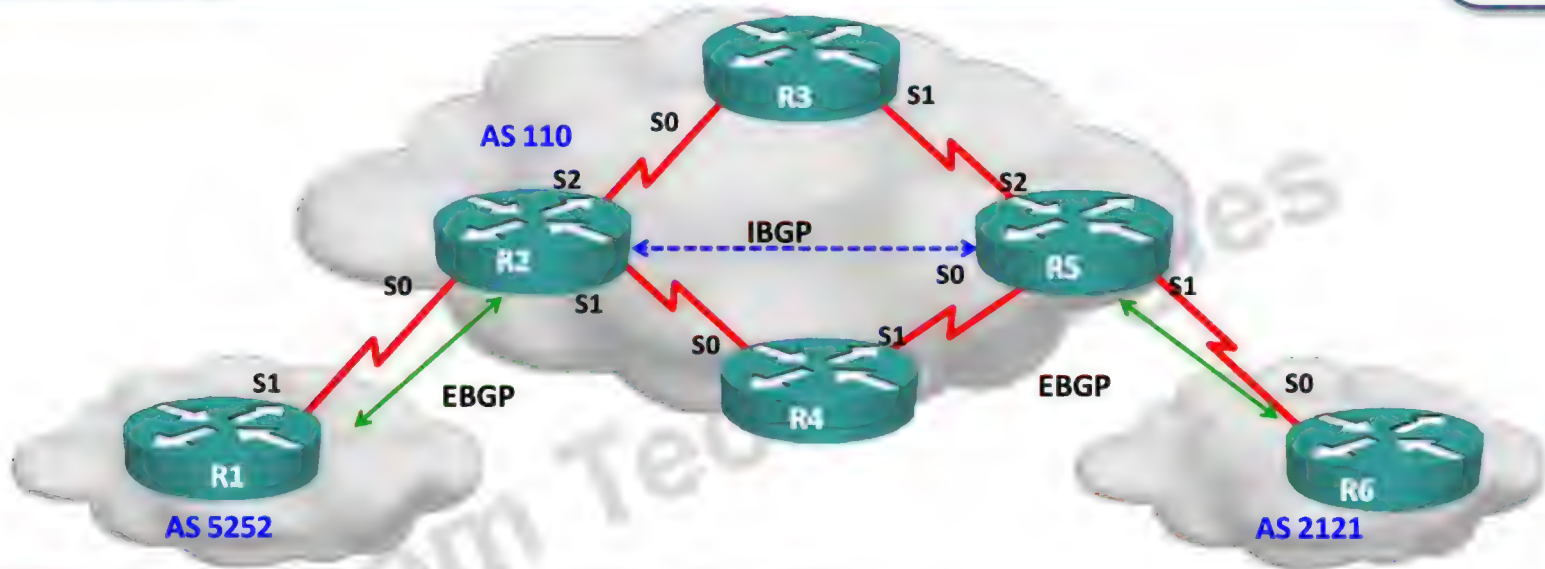
Update

Notification



- BGP neighbors are routers forming a TCP connection for exchanging BGP updates. Also called as BGP Peers or BGP Speakers.
- Two type of BGP neighbor relationship.
 - IBGP (Internal BGP)
 - EBGP (External BGP)





IBGP: Router Forming neighbor relationship within A.S.
IBGP neighbors doesn't need to be directly connected

EBGP: Router Forming neighbor relationship between two different A.S.
EBGP neighbors need to be directly connected – though there may be exceptions to this



Configuring BGP Routing Protocol

```
Router(config)# router bgp <AS no.>
```

Configuring BGP Routing Protocol

```
Router(config-router)# network <network ID>  
[mask <subnet mask>]
```

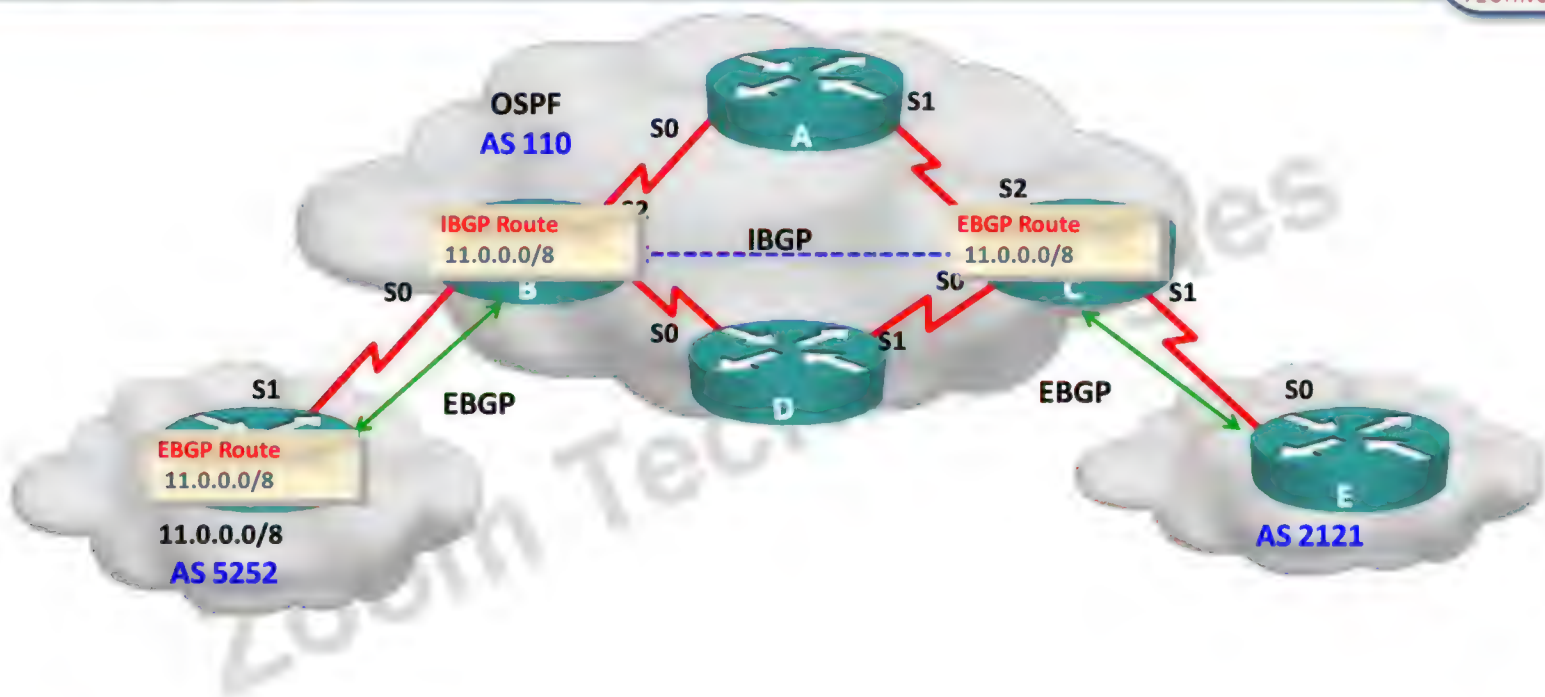
- Only one instance of BGP per Router
- Same network prefix must exist in routing table
- Network may not be directly connected
- Network without subnet mask will take classful mask

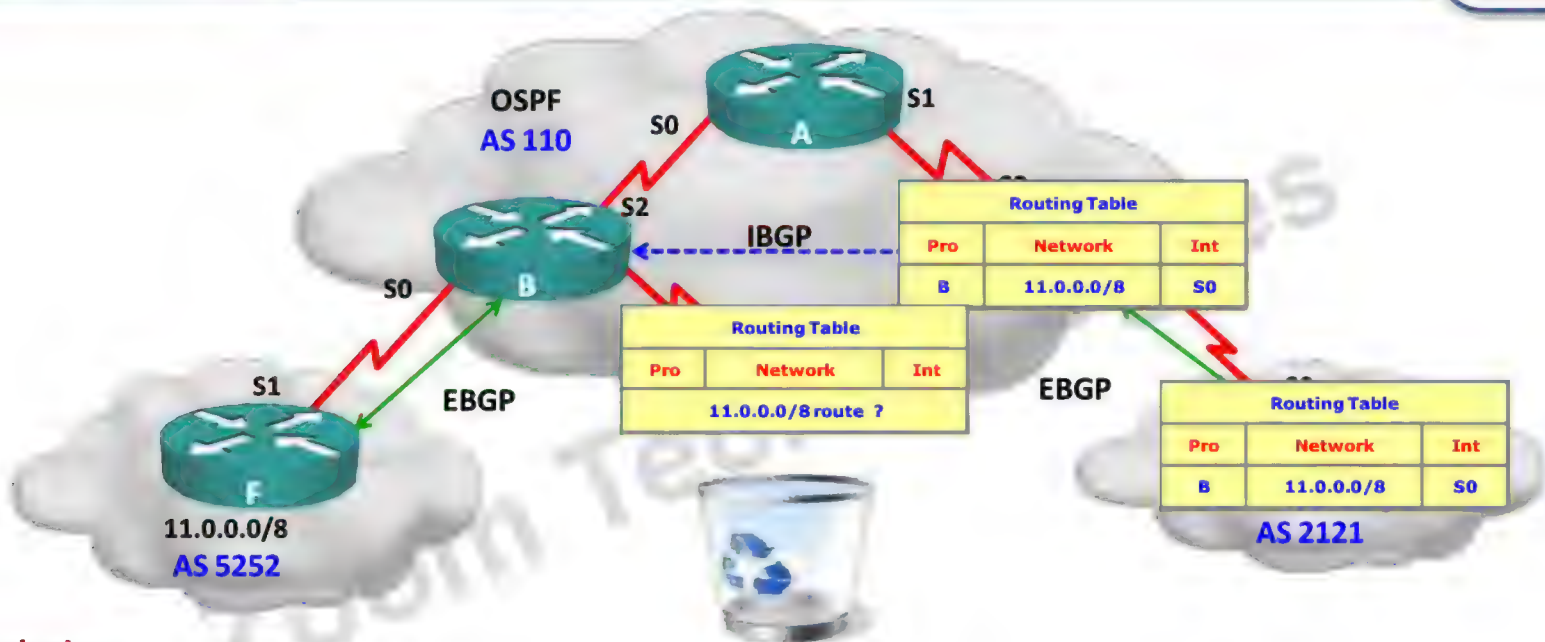


Configuring BGP Routing Protocol

```
Router(config-router)# neighbor <IP-Address>
remote-as <AS No.>
```

- Router should have a route in the normal routing table to reach neighbor
- Same command for IBGP and EBGP neighbor, only the AS number will be different for an EBGP neighbor.



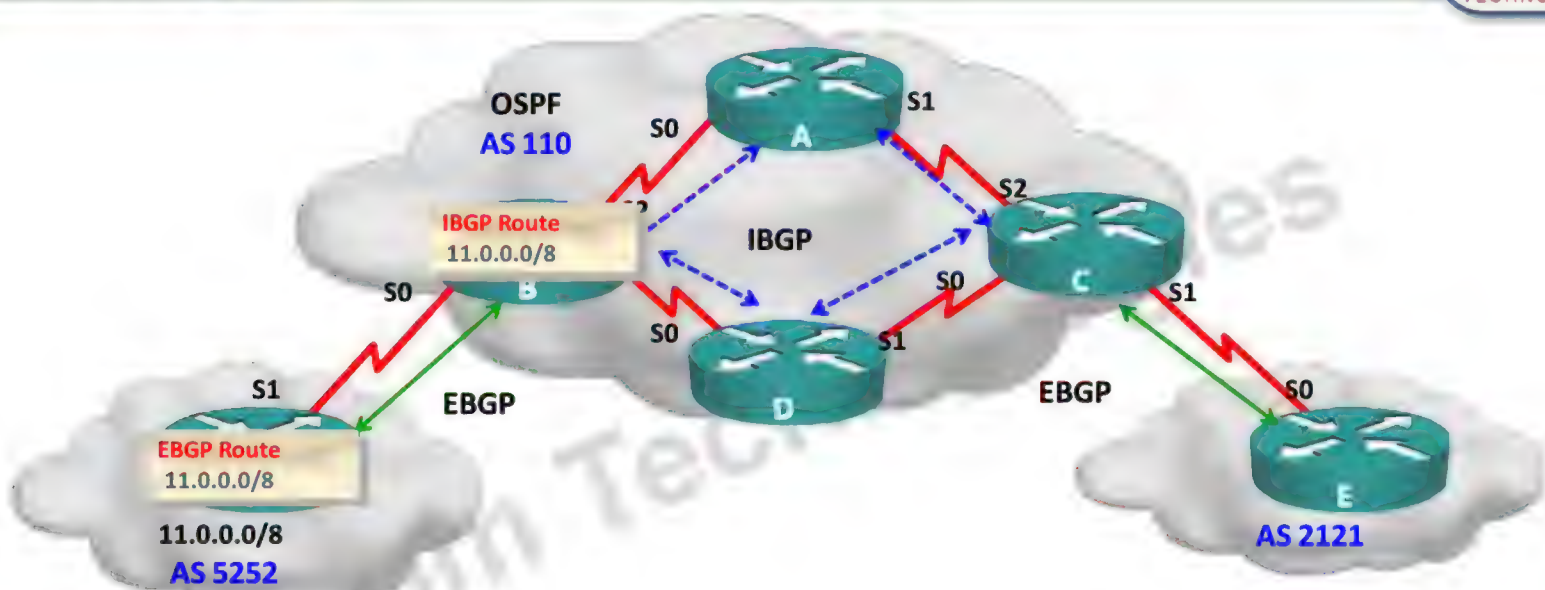


Solution :

- Redistribute BGP into IGP (Not recommended)
- Run BGP on All transit routers (routers coming in path from one A.S to other)



Split Horizon in BGP

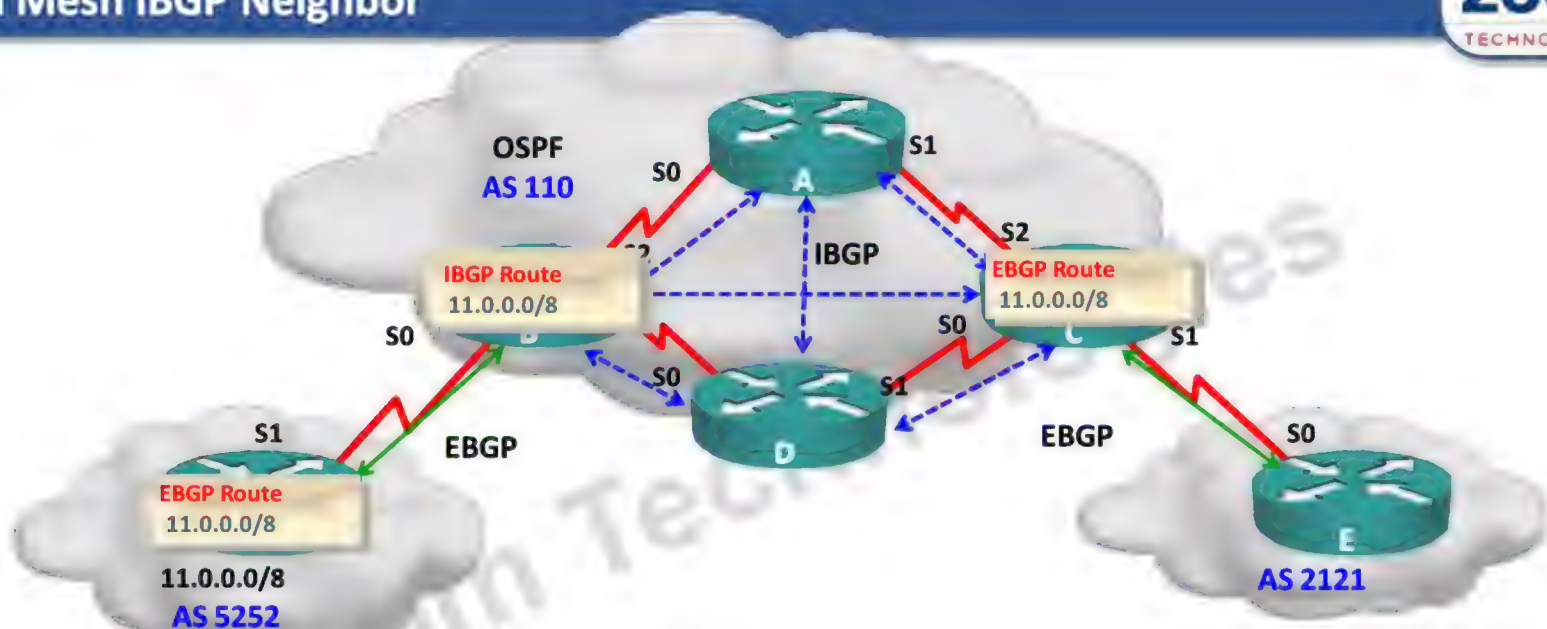


Split Horizon :

- Updates coming from IBGP neighbor cannot be forwarded to other IBGP neighbors



Full Mesh IBGP Neighbor

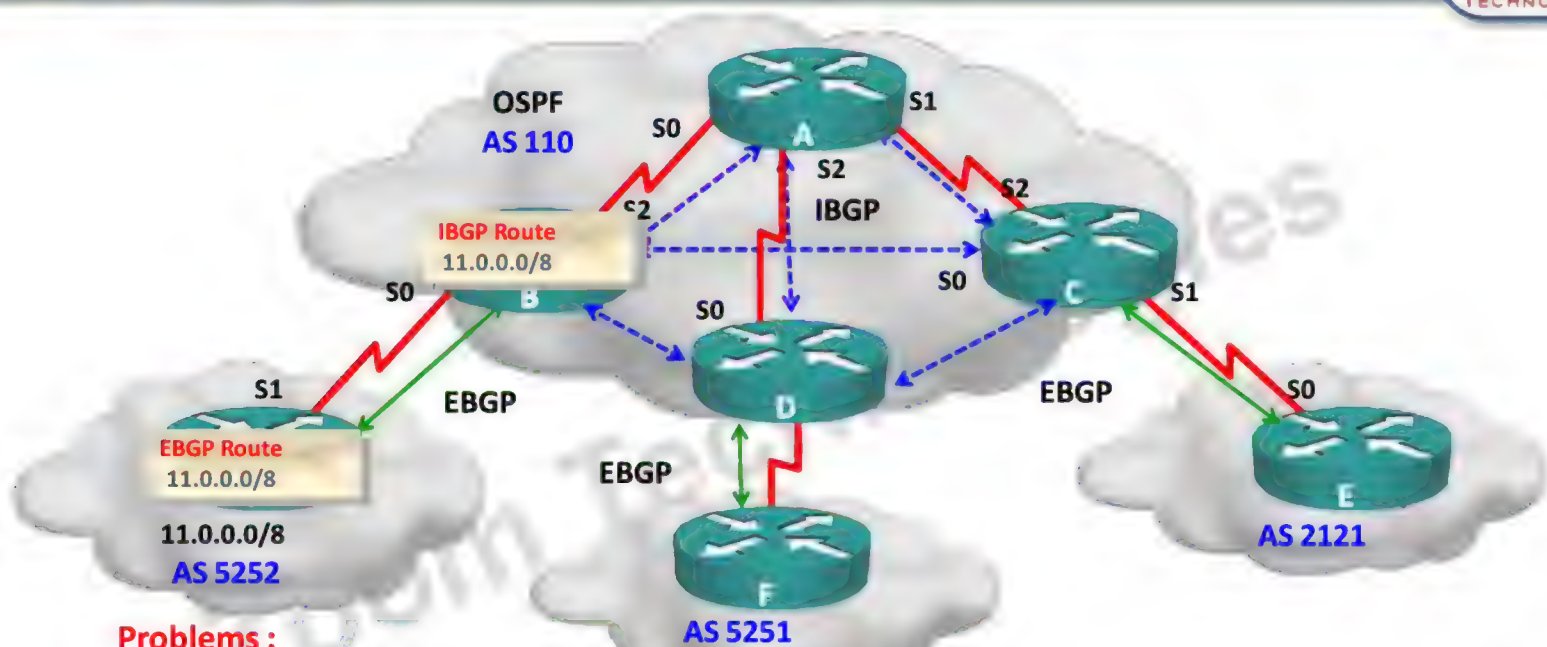


Solution:

- Configure full mesh IBGP neighbor relationship OR
- Use Route Reflector



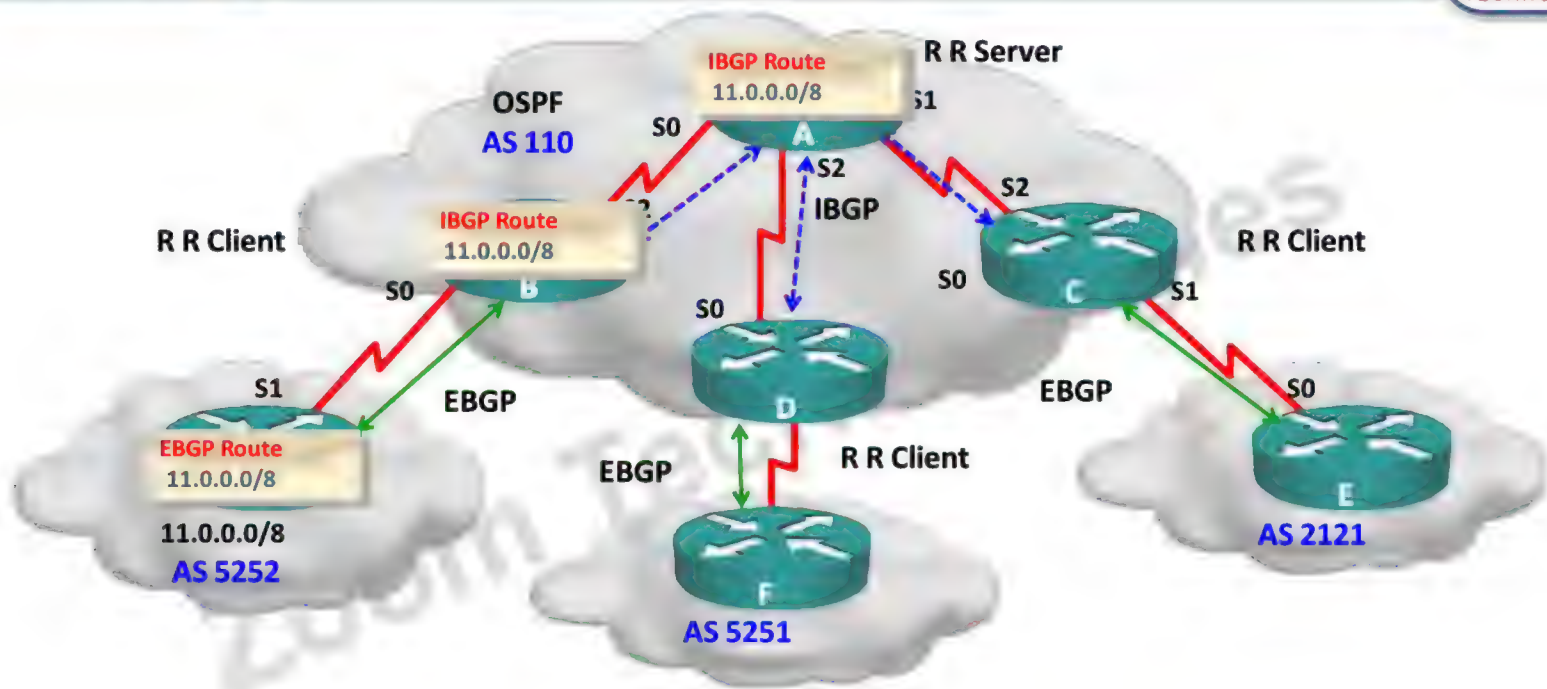
BGP - Star Topology



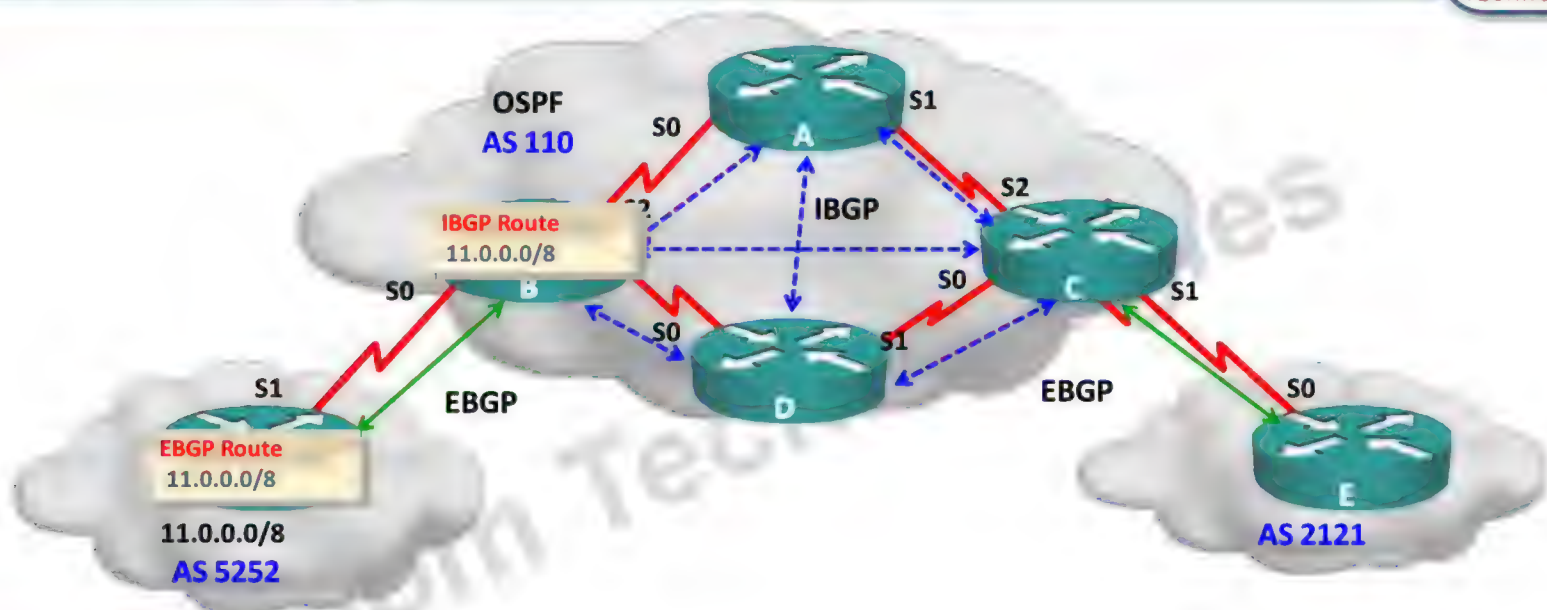
Problems :

- In Star topology same routing updates to different router need to pass through hub router
- This creates repetition of same updates
- BGP in full mesh creates $(n \times (n - 1)) / 2$ IBGP Neighbor relationship



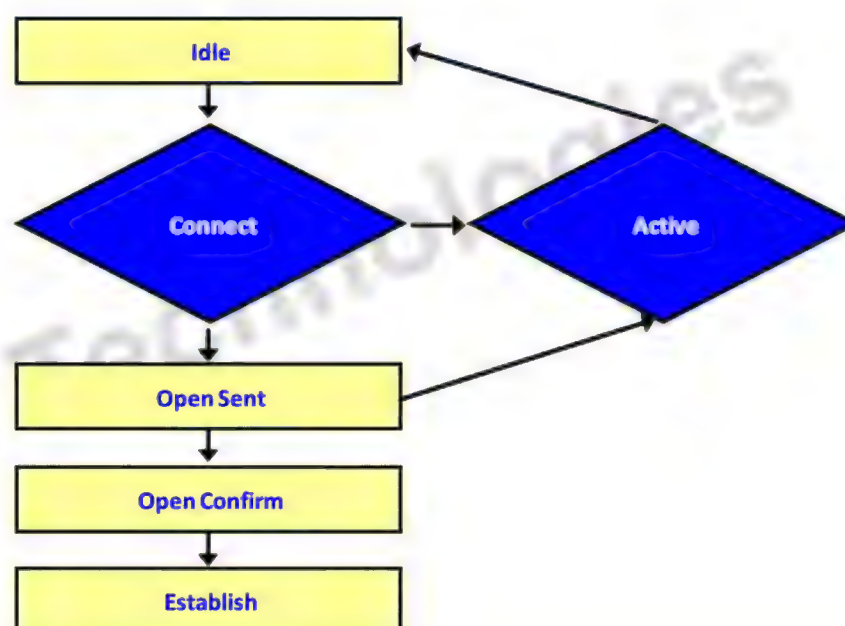


- A Route Reflector is one method of disabling Split Horizon in BGP.
- By using Route Reflector, routers are divided into two roles
 - 1) Route Reflector Server
 - 2) Route Reflector Client
- Route Reflector client will update server, then server will update remaining clients.



BGP Synchronization Rule :

- If updates are received from IBGP neighbor, it cannot be used in routing table nor sent to other EBGP neighbor till same update comes from Interior Gateway Protocol.

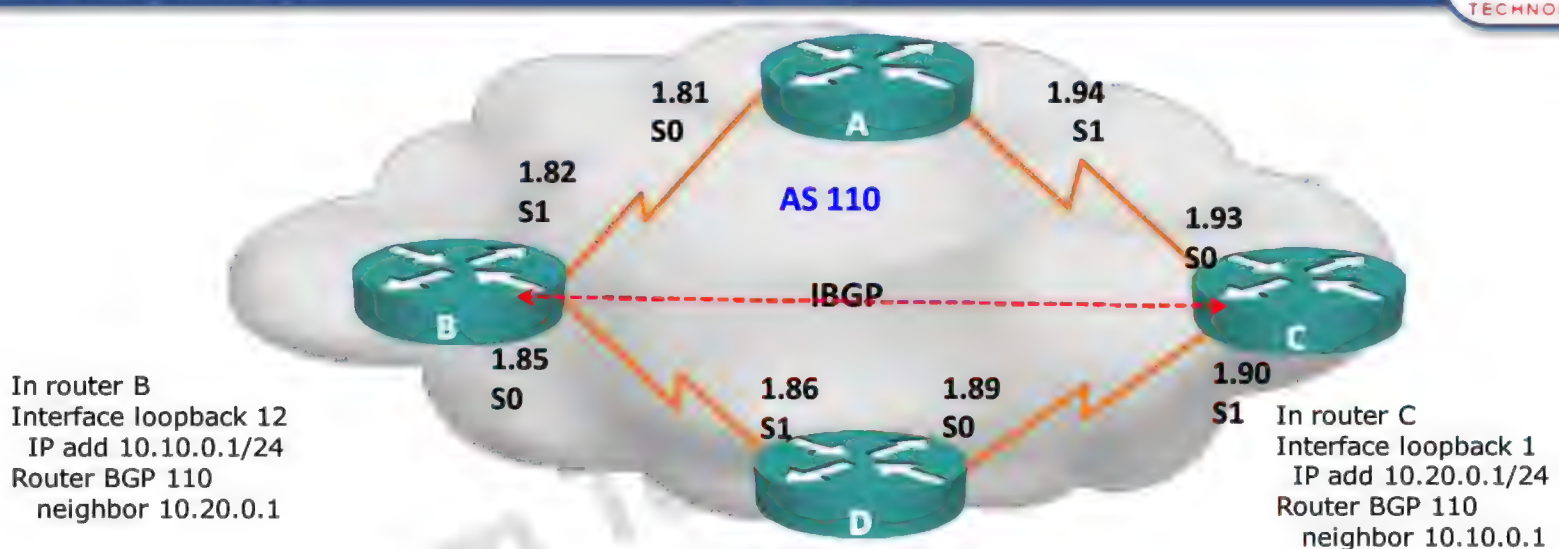


Border Gateway Protocol (BGP - Day -2)

ZOOM

BGP Neighbor

ZOOM
TECHNOLOGIES



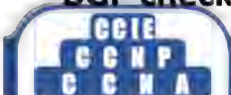
Loopback interface should be used for forming neighbor relationship.

BGP messages

Destination IP = Neighbor IP

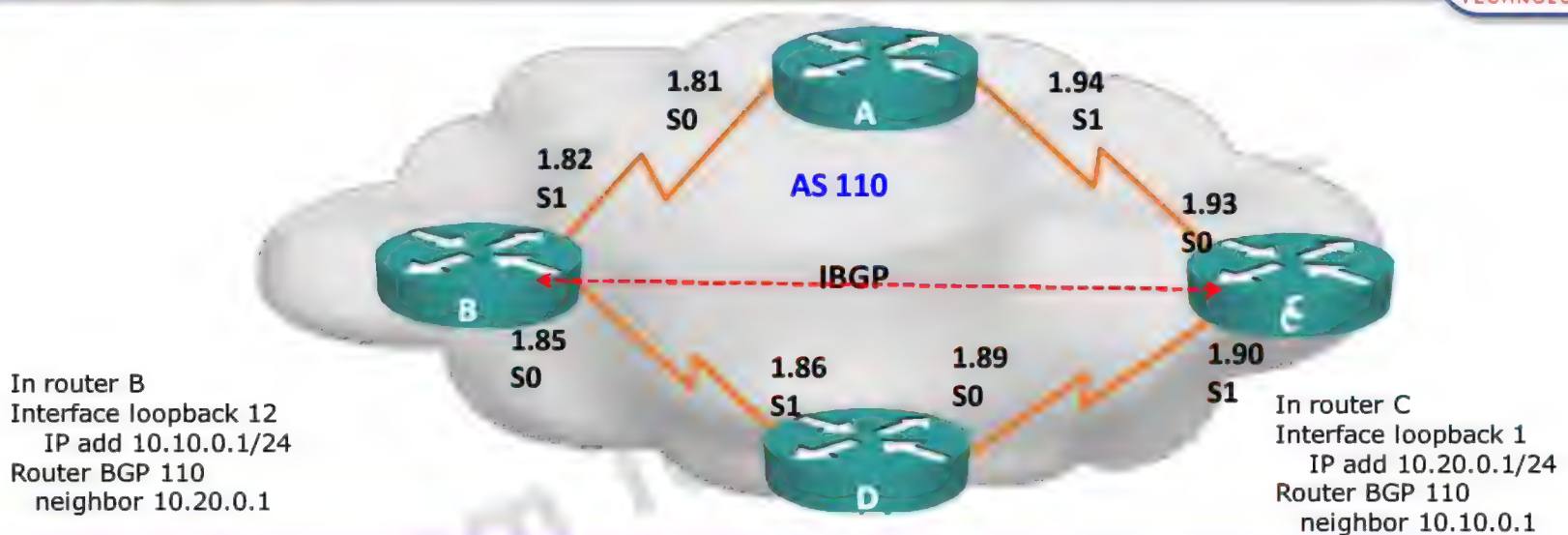
Source IP = Primary IP of Outgoing Interface

BGP check source IP in its neighbor command, if no match Message will be discarded.



BGP Neighbor

ZOOM
TECHNOLOGIES



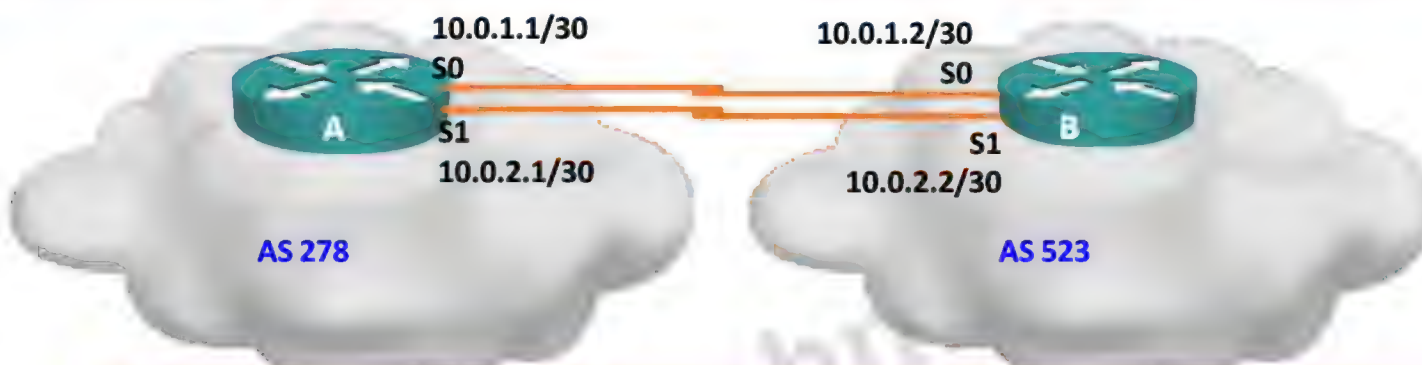
On Router B

```
B(config)#router BGP 110
B(config-router)#neighbor 10.20.0.1 remote-as 110
B(config-router)#neighbor 10.20.0.1 update-source loopback 12
B(config)#int loopback 12
B(config-if)#ip add 10.10.0.1 255.255.255.0
```

CCNP
CCNA

EBGP Neighbor

ZOOM
TECHNOLOGIES



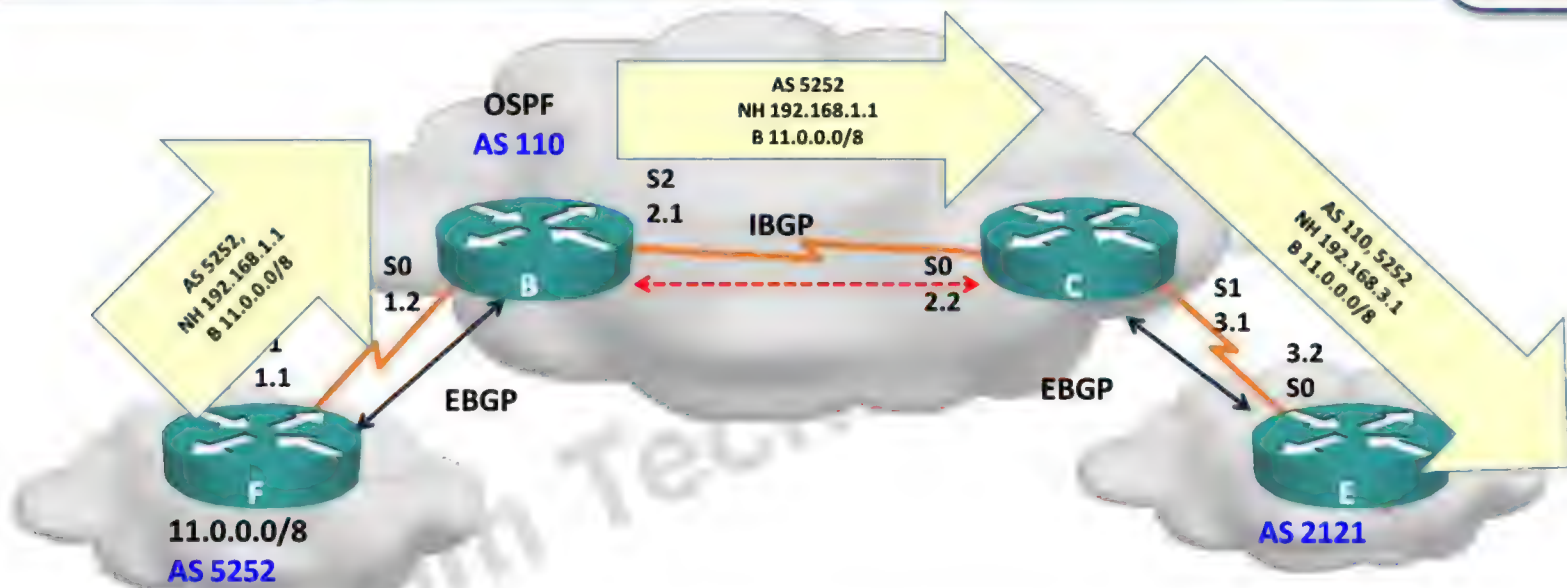
On Router A

```
A(config)#router BGP 278
A(config-router)#neighbor 10.20.0.1 remote-as 523
A(config-router)#neighbor 10.20.0.1 update-source loopback 12
A(config-router)#neighbor 10.20.0.1 ebgp-multihop 2
A(config)#int loopback 12
A(config-if)#ip add 10.10.0.1 255.255.255.0
A(config)#ip route 10.20.0.0 255.255.255.0 s 0
A(config)#ip route 10.20.0.0 255.255.255.0 s 1
```

CCNP
CCNA

Next Hop in BGP

ZOOM
TECHNOLOGIES



BGP is an AS-by-AS routing protocol, not a router-by-router routing protocol.

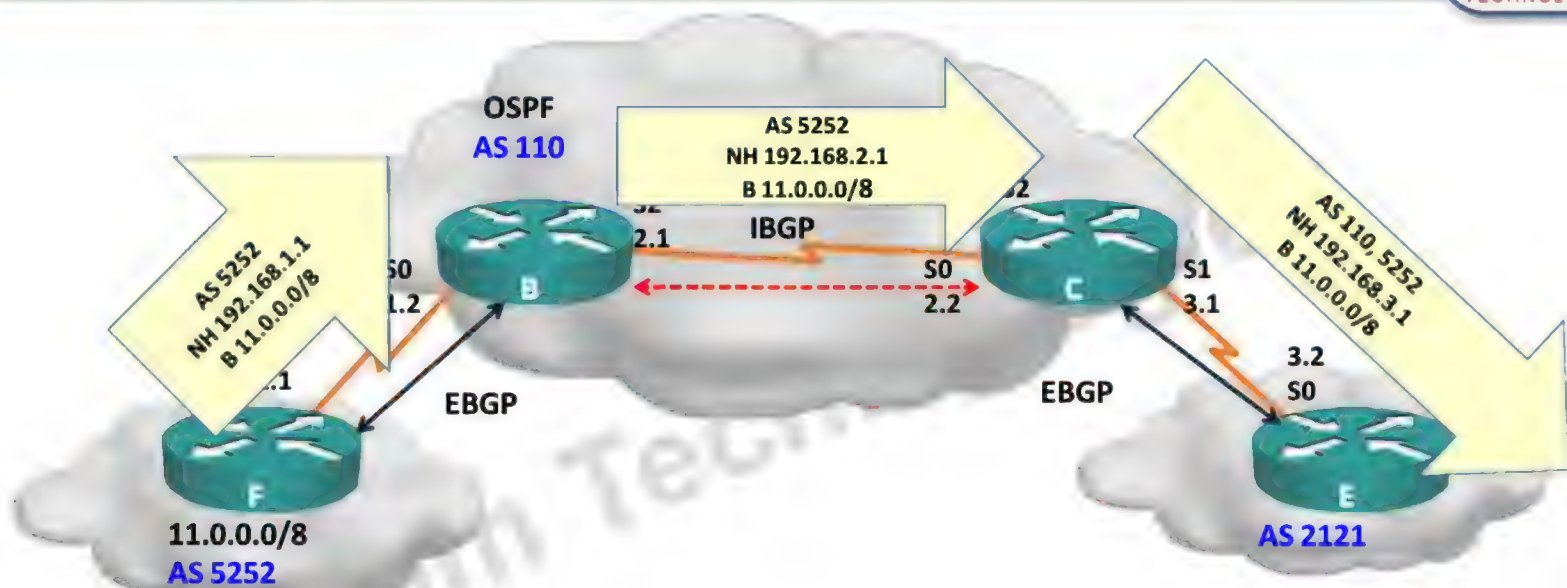
next hop \neq next router,

the Next-hop IP address used to reach the next AS.



Next Hop in BGP

ZOOM
TECHNOLOGIES



If Router C doesn't know how to reach 1.1 it cannot reach 11.0.0.0 network.

B(config-router)#neighbor 192.168.2.2 next-hop-self



- **Clearing BGP neighbor relationship**
- On modification or implementation of new policy, BGP takes time to show results. For instant implementation of policies, resetting BGP peers is required.
- **R#clear ip bgp * | <neighbor IP>**
- BGP resets connection and starts from Idle State.
- **R#clear ip bgp * | <neighbor IP> soft out | in**
- Clears only BGP updates, TCP connection will not be reset.
- If BGP State is Idle or Active for long time.
- Check for neighbor command in both routers.
- Check whether a route exists in routing table to reach neighbor.



- BGP Supports auto and manual summary.
- Manual summary can be done at any point in network.
 - Summary can carry network belonging to multiple A.S.

R(config-Router)#aggregate-address <network> <mask> [summary-only]



BGP Authentication



- BGP supports MD-5 authentication.
- Configure a “key” (password); router generates a message digest, or hash, of the key and the message.
- Message digest is sent; key is not sent.

```
Router(config-router)# neighbor <neighbor IP address> password <string>
```



BGP Metric



- BGP metrics are called Attributes or Rich Metrics.
- BGP attribute types:
 - Well Known
 - Recognized by all the vendors.
 - Optional
 - May not be recognized by every vendor
 - Mandatory
 - Must be present in all updates.
 - Discretionary
 - May be present or not in updates
 - Transitive
 - Must be sent to other neighbors.
 - Non transitive
 - Only for that router. Should not be passed to neighbors.
 - Partial
 - Proprietary



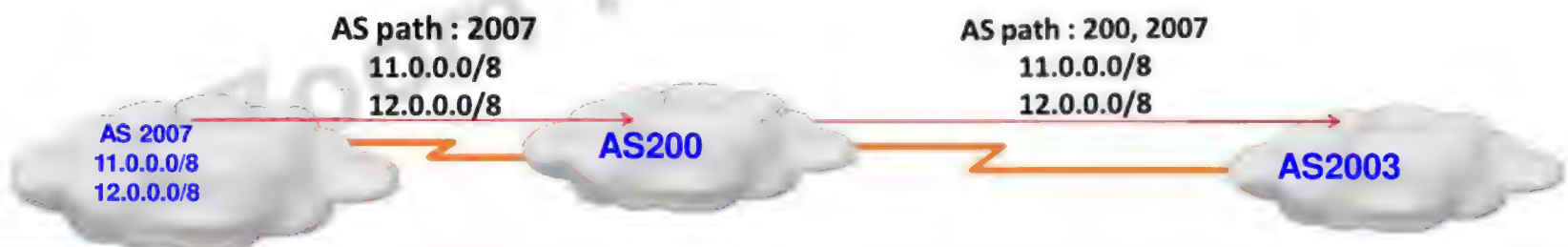
BGP Attributes

- Some BGP Attributes :
- AS Path
- Next hop
- Origin
- Local preference
- Multi Exit Discriminator
- Weight

Zoom Technologies

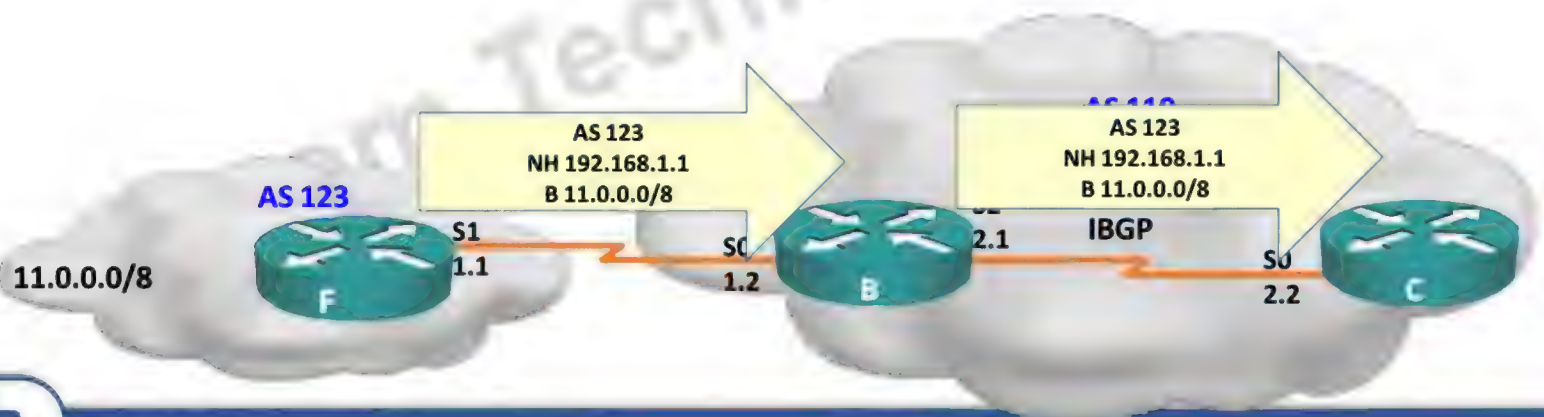
AS Path

- AS Path : List of AS through which updates has traversed.
- Path with shortest AS path list is more desirable.
- AS Path is a well known, mandatory and transitive attribute.



Next Hop

- BGP is AS by AS routing Protocol
- Next hop \neq next router
- Next hop = IP to reach next AS
- Next hop well known, mandatory and transitive attribute.



Origin

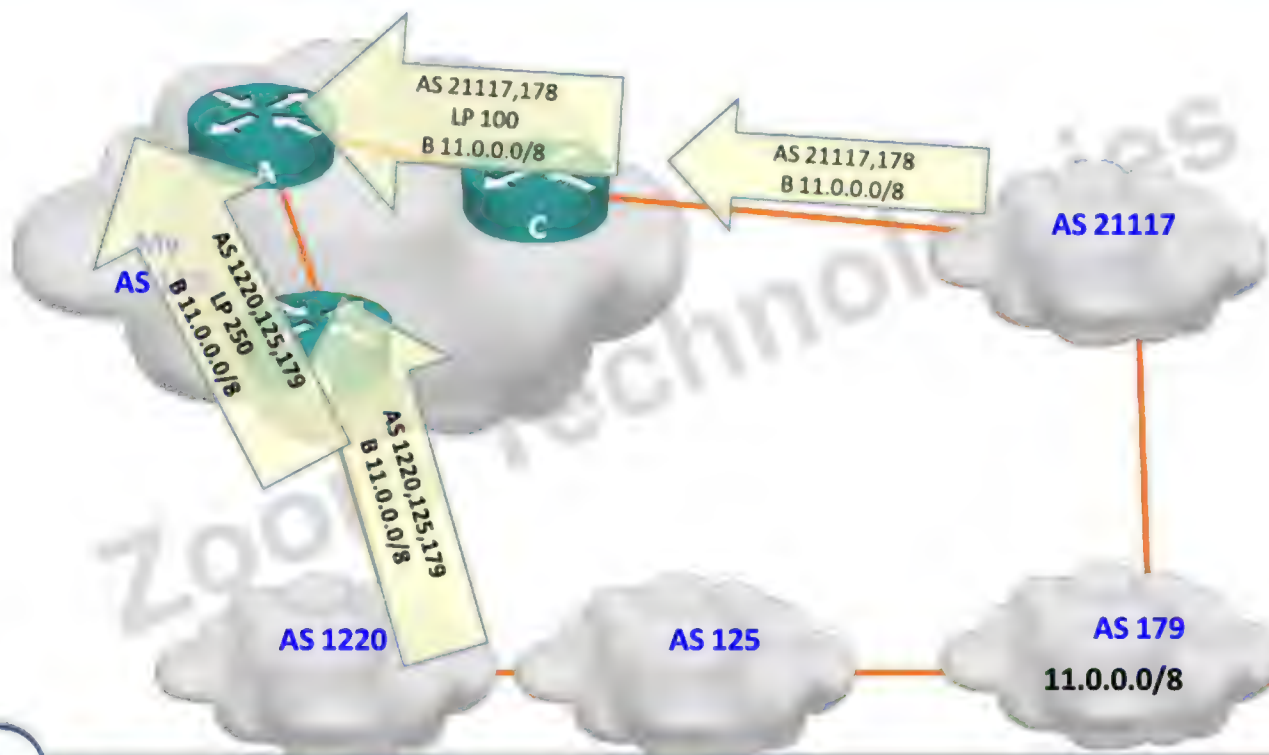
- Origin informs all ASs in Internetwork how network got introduced into BGP.
 - IGP (i)
 - network command
 - EGP (e)
 - Redistributed from EGP
 - Incomplete (?)
 - Redistributed from IGP or static
- The origin attribute is well-known, mandatory, and transitive.
- "I" is better than "e" and "e" is better than "?"

Local Preference

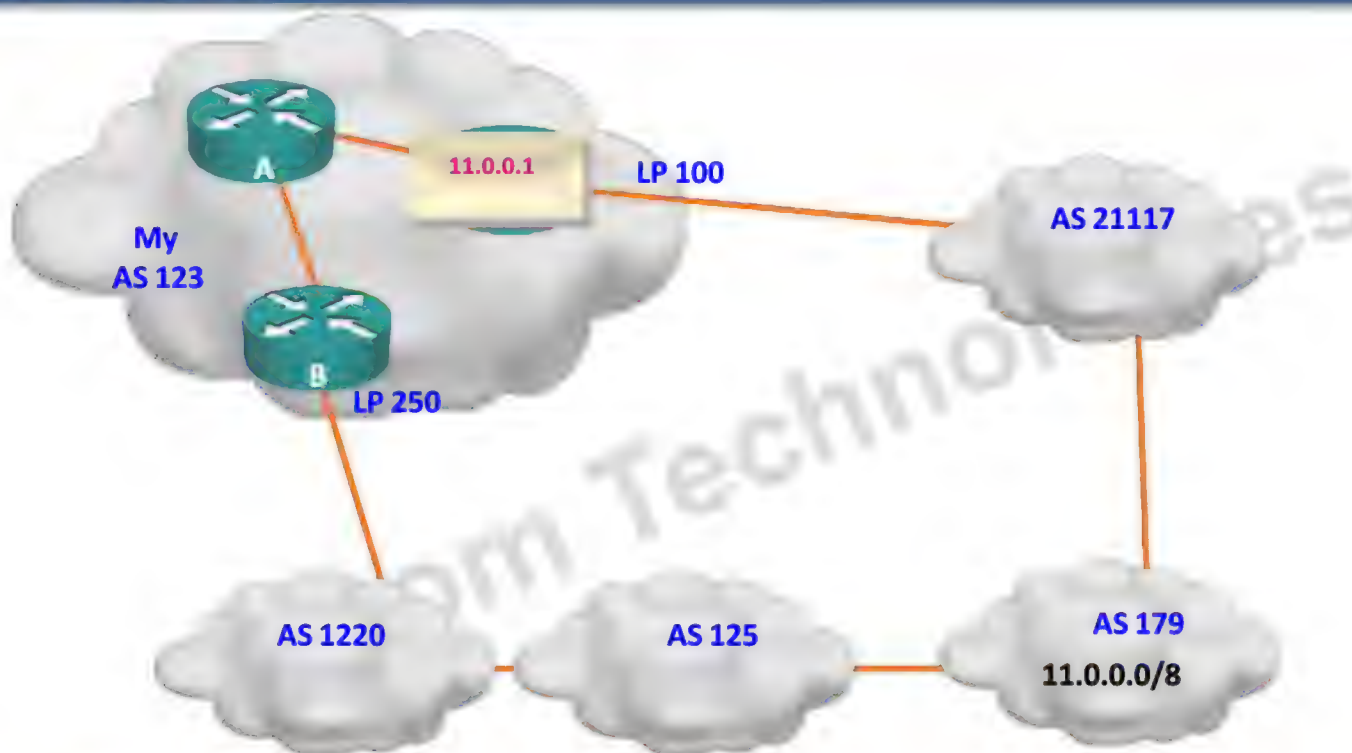
- Local preference defines how data traffic should exit from an AS.
- Default value is 100
- Path with highest preference value is more desirable.
- It is advertised only to IBGP neighbor within an AS.
- Local preference is Well known, discretionary and transitive only to IBGP neighbor.

Zoom Technologies

Local Preference

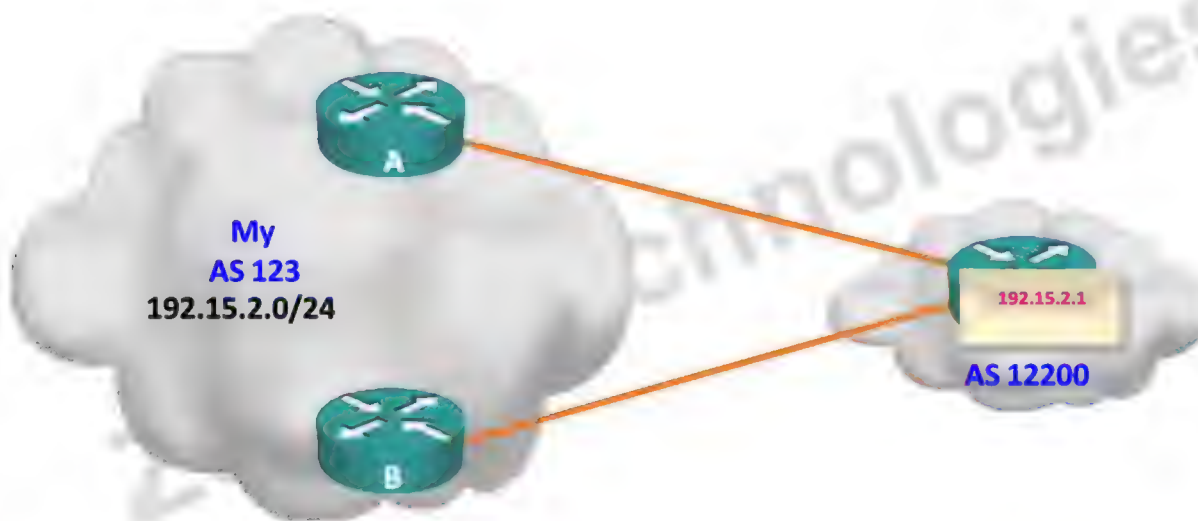
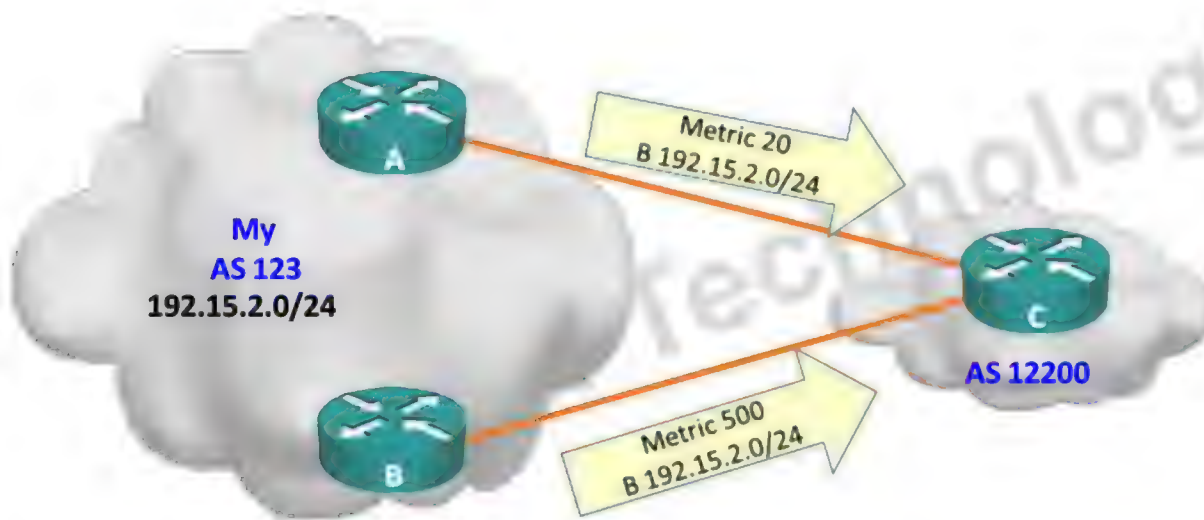


Local Preference



MED

- MED define how the data traffic should enter an AS.
 - Default is value 0.
 - Path with less MED is more desirable.
 - MED is used to advertised to EBGP neighbor only.
 - MED is optional and non transitive
- Zoom Technologies

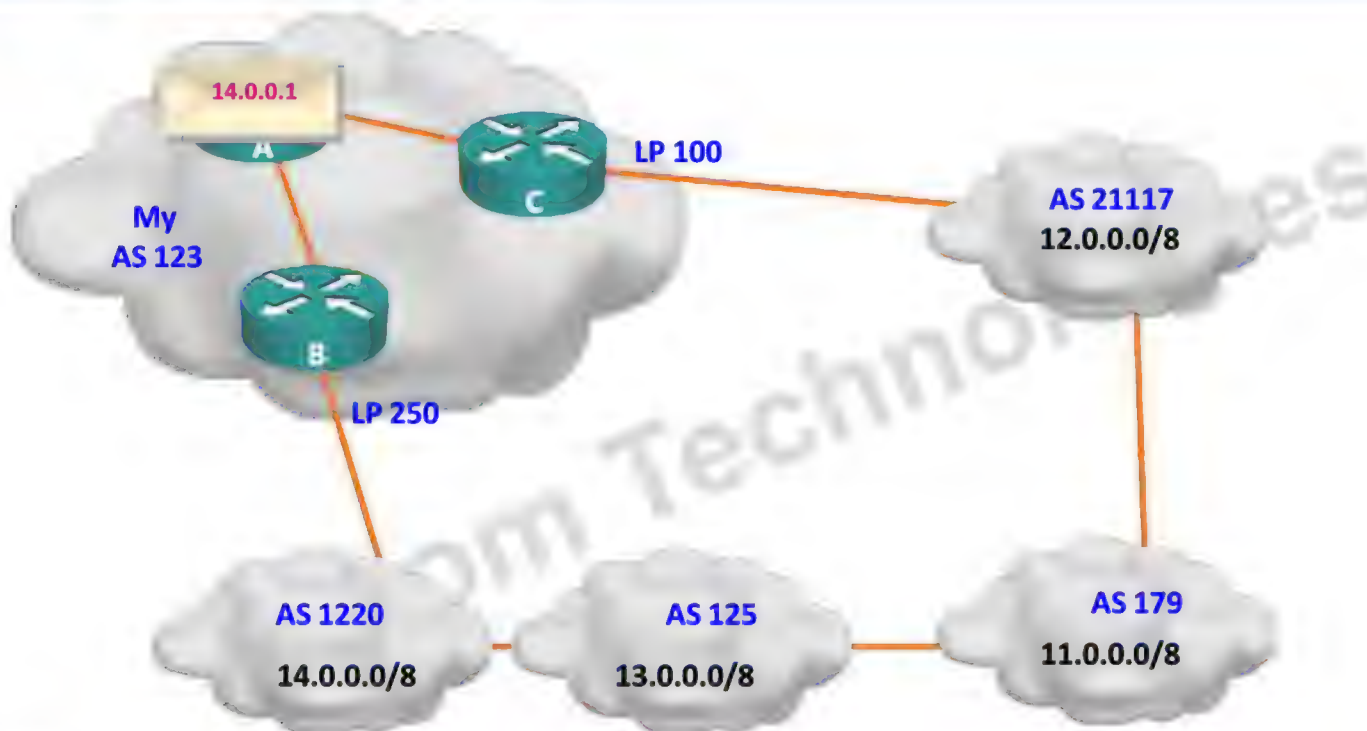




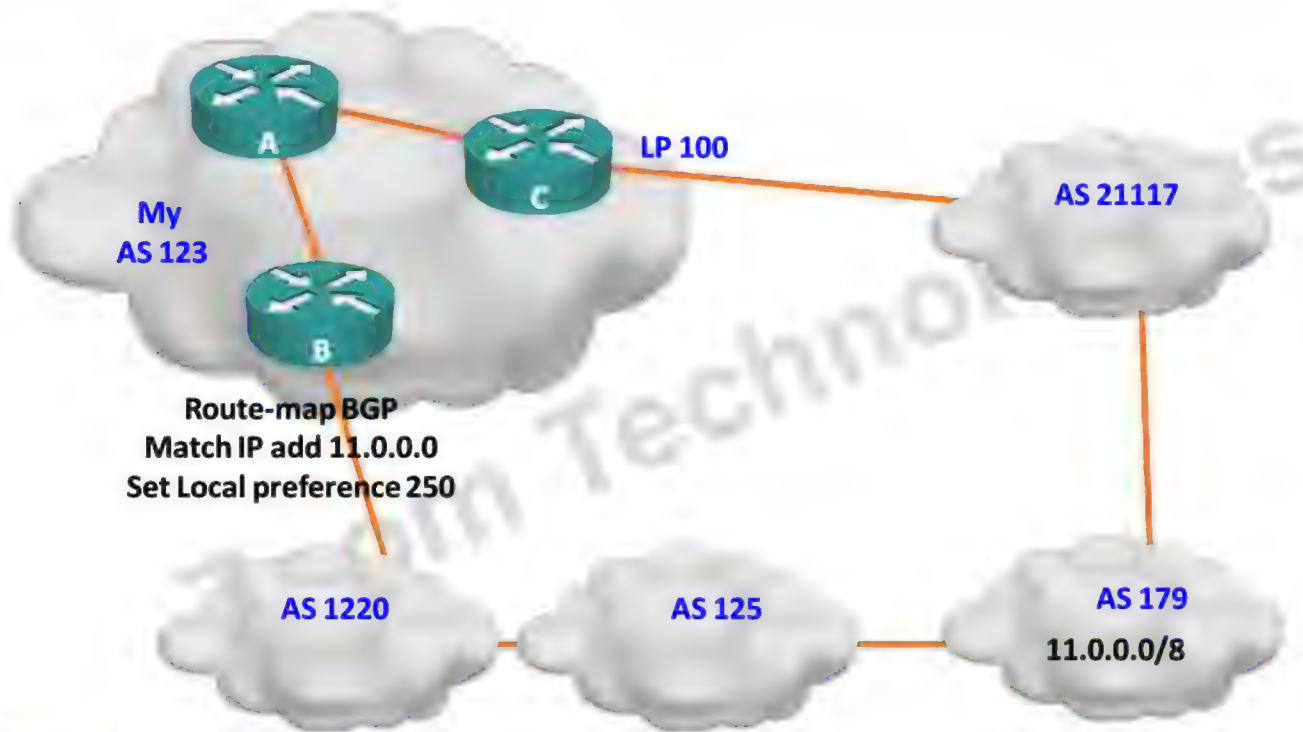
- Weight is Cisco's attribute.
- Path with the highest weight is more desirable.
- Default weight is 32768 for local network and 0 for other.
- Weight is configured locally to each router, it is not advertised to any neighbor.
- Weight is partial attribute.

BGP Consider only (synchronized), no AS loops and a valid next hop route for path selection processes:

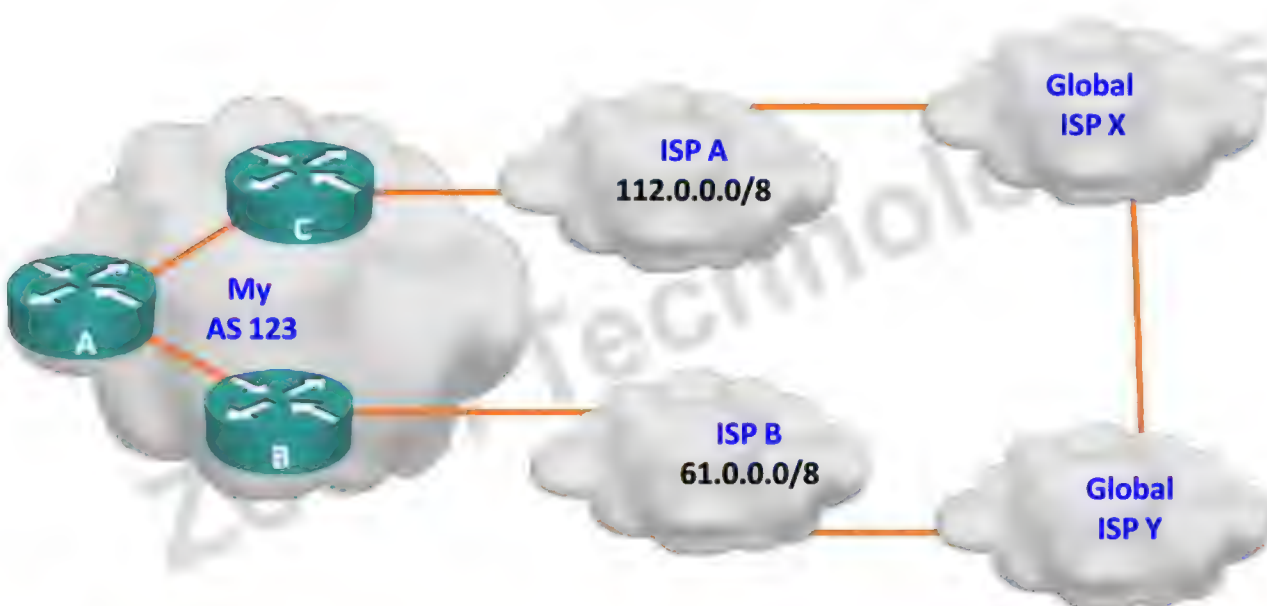
- Prefer highest weight (local to router)
- Prefer highest local preference (global within AS)
- Prefer route originated by the local router (next hop = 0.0.0.0)
- Prefer shortest AS path
- Prefer lowest origin code (IGP < EGP < incomplete)
- Prefer lowest MED (from other AS)
- Prefer a path from EBGP neighbor over IBGP neighbor
- Prefer the path through the closest IGP neighbor
- Prefer oldest route for EBGP neighbor
- Prefer the path with the lowest neighbor BGP router ID



Route Map for BGP policy



Multi-homing AS





Why Do We Need IPV6

ZOOM
TECHNOLOGIES

BBC Mobile | Home | Sport | Weather | Travel | TV | Radio | More

NEWS TECHNOLOGY

Home | UK | Africa | Asia-Pac | Europe | Latin America | Middle East | South Asia | US & Canada | Business | Health | Science/Environment | Tech | Entertainment | Video

4 February 2011 Last updated at 13:23 GMT

Last blocks of net addresses get handed over

The original pool of internet addresses has officially run dry.

The last five blocks of the IP Version 4 addresses have been handed over to the regional bodies that distribute them.

Those five blocks, called /8s and which contain 16 million addresses each, are expected to be completely depleted by September 2012.

The move to the new addressing scheme, known as version 6, is under way but will take years to complete.

"This is one of the most important days in the internet's history," said Rod Beckstrom, Internet overseer Icaann at a press conference called to mark the handing over of the final five blocks.

"It is a point that the founders of the internet thought would occur far in the future," he said. "It gives us an opportunity to shift to an internet protocol that offers a pool so large that it is difficult even to imagine."

IPv6 has a pool of addresses a billion, trillion times larger than the 4.3 billion that IPv4 can support.

While that pool of 4.3 billion addresses was seen as plenty when the internet was first created, it is now running out.

Top Stories

- New call to oust Egypt's Mubarak
- Chechen claims airport bombing
- Philippines ex-army chief suicide
- Hague on 'reform tour' in Tunisia
- First Korean talks since shelling

Features & Analysis

- Known and unknown**
US media react to ex-US defence chief Donald Rumsfeld's memoirs
- New nation**
Southern Sudanese celebrate independence result
- Reaching for the sky**
Grand plans for high-rise buildings inch forward in Cambodia
- Fossil forests**
Scientists claim ancient woodlands could provide clues to the future

Related Stories

- Last net addresses to be shared
- Net approaches address exhaustion
- Tuning in to the background hum of the net

CCIE
CNP
CCNA

No More IPv4 Addresses!

Why Do We Need a Larger Address Space?

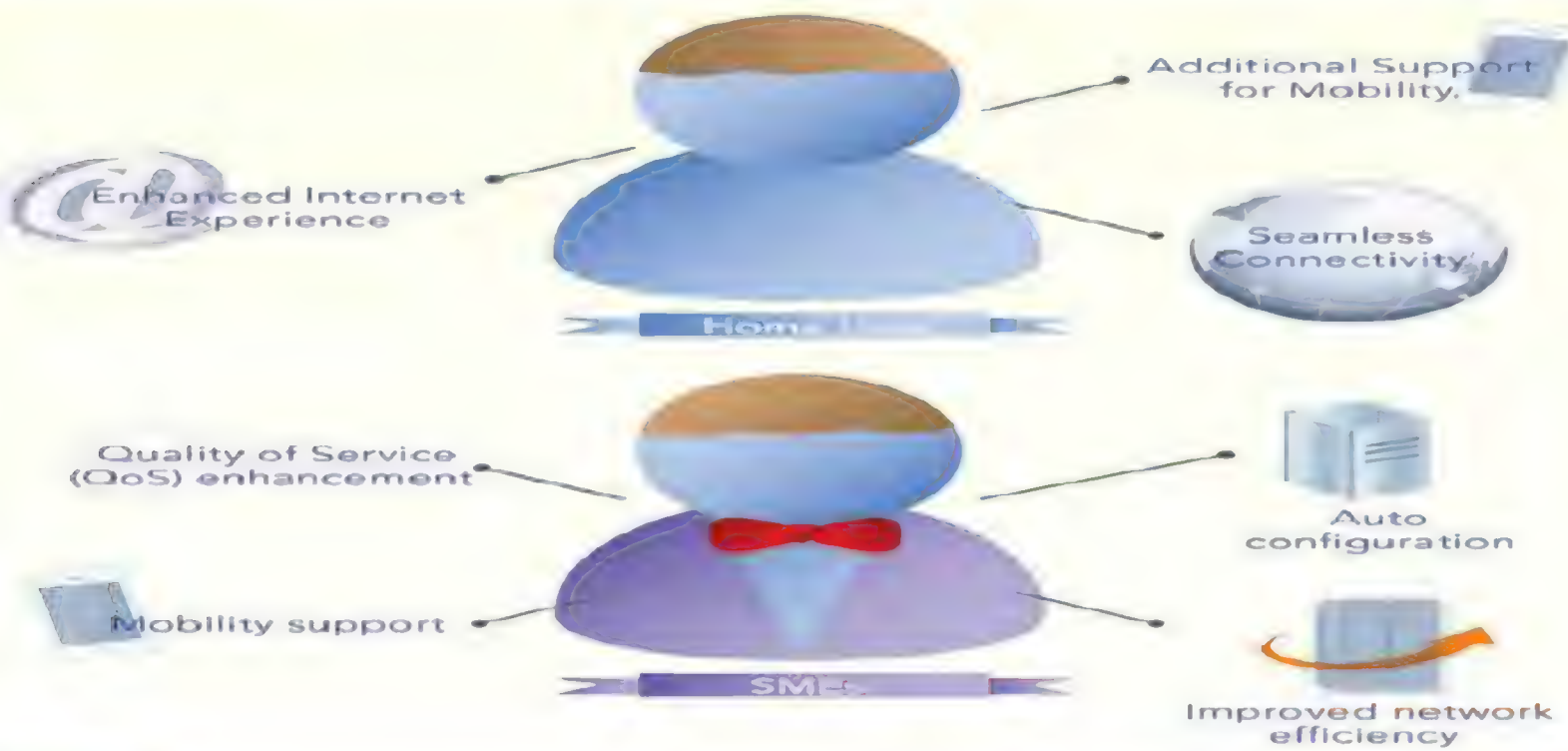
- Internet population has grown exponentially
- Millions of Mobile users
- Transportation
- Consumer devices
- No. of Websites - again exponential growth

IPV4 vs IPV6

Features	IPv4	IPv6
Notation	Dotted Decimal Notation Example: 10.0.1.100	Hexadecimal Notation with Colon Example: 2001:03BB:B5A1:52FF: FEA5:4564:0112:1202
Address Size	32-bits	128-bits
Number of Address	$2^{32} =$ 4,294,967,296 Addresses	$2^{128} =$ 340,282,366,920,938,463,463,374,607,431,768, 211,459 Addresses
Packet Broadcast	- Support broadcasting	- No broadcasting, IPv6 using multicast.

IPv6 Advantages

ZOOM
TECHNOLOGIES



CCNP
CCNA

IPv4 vs IPv6

ZOOM
TECHNOLOGIES

IPv4

ADDRESS - 32 BITS
203.121.111.123

IPv6

ADDRESS - 128 BITS
2001:0ab8:85a3:0000:0000:6a2e:0370:7334

CCIE
CCNP
CCNA

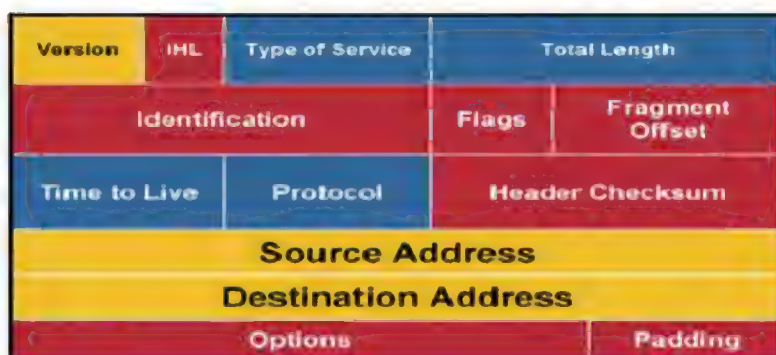
IPv6 Address Representation

- IPv6 Format : x:x:x:x:x:x:x
- where x is 16 bits Hexadecimal
- Leading zeros in a x field are optional
- Successive x Fields of 0 can be represented as :: but only once
- Eg. 2031:0000:0000:013f:0000:0000:0000:0001

Zoom Technologies

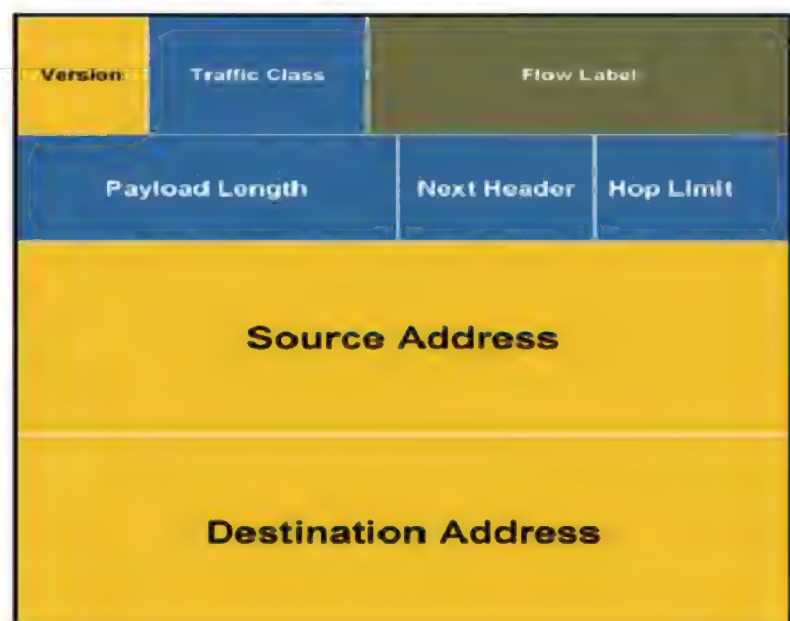
IPv4 and IPv6 Header Comparison

IPv4 Header



- Field name kept from IPv4 to IPv6
- Fields not kept in IPv6
- Name and position changed in IPv6
- New field in IPv6

IPv6 Header



IPv6 Address Type



- Unicast
- Multicast
- Anycast

Zoom Technologies



Unicast

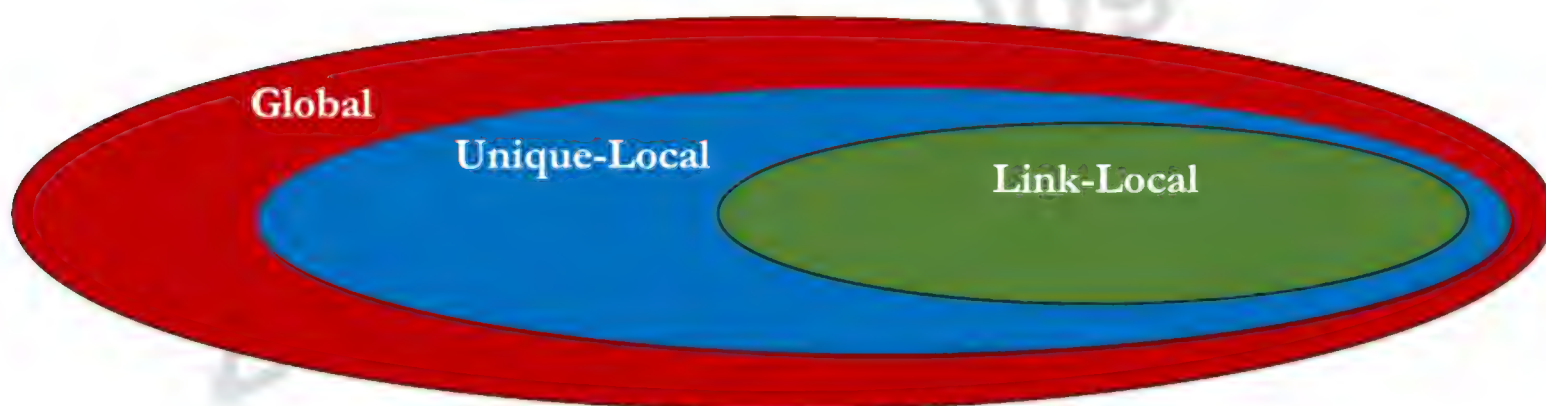


- There are three type of unicast address
 - Global Unicast
 - Unique Local
 - Link-Local

Zoom Technologies



Address Scope



- Allows computers to communicate on the internet.
- The Internet Assigned Numbers Authority (IANA) delegates the current global address's prefix as 2000::/3.

Link Local



- Enables communication within local link (local physical network) only.
- Equivalent to Automatic Private IP Addressing (APIPA)
- The first 10 bits of link-local IP address is set to 111111010, which is equals to FE80 when it is converted to hexadecimal.
- A link-local IP address is always begins with FE80.

Zoom Technologies



Unique Local

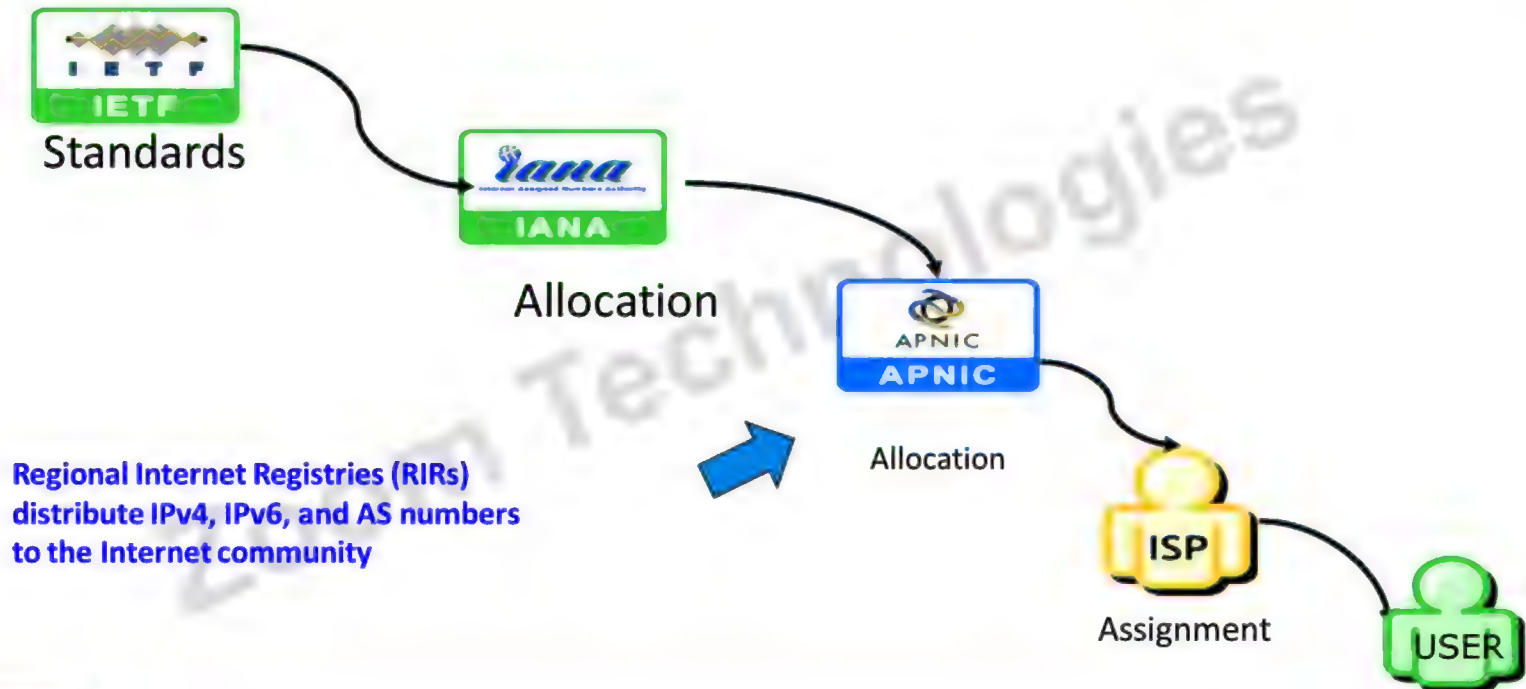


- Equivalent to private IPv4 addresses
- Packets are routed within an organization , and not outside it on the public internet.
- In IPv4, these addresses are 10.0.0.0/8, 172.16.0.0/12 and 192.168.0.0/16.
- IPv6's site-local addresses have set the first 10 bits to 111111011, which equals to FC00.

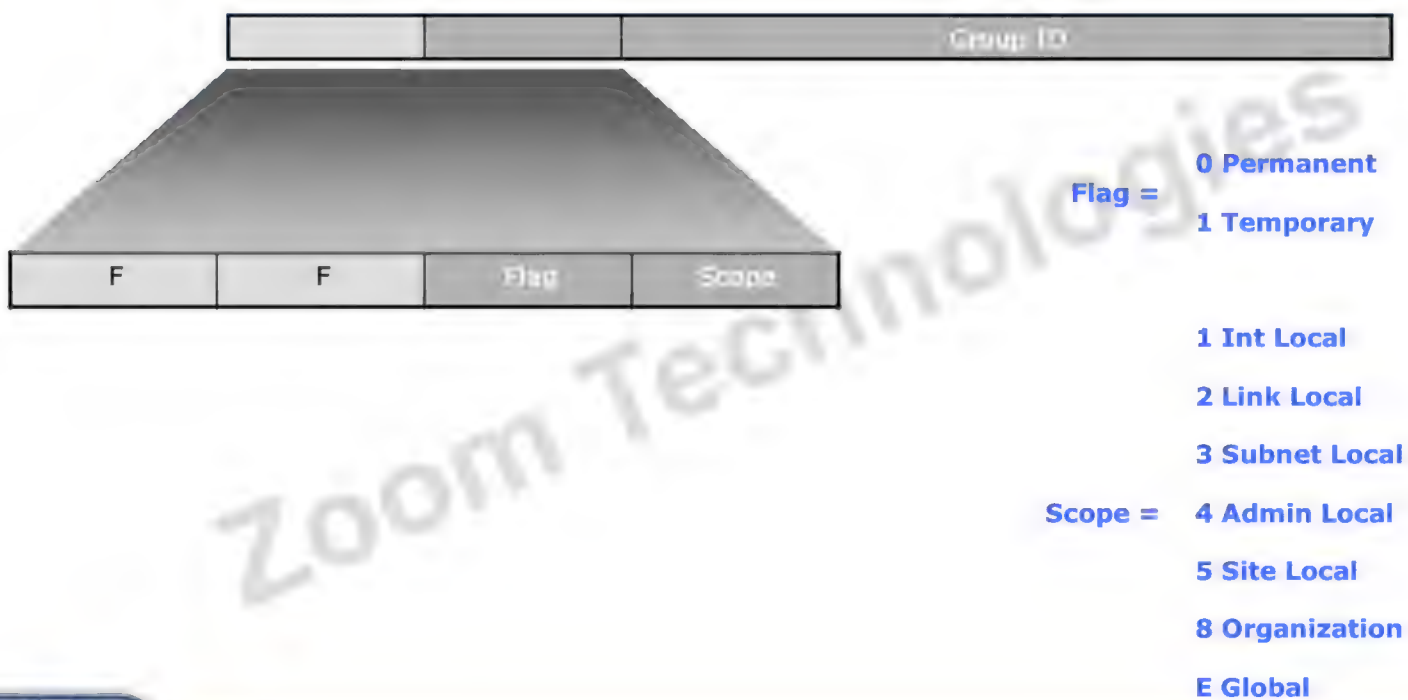
Zoom Technologies



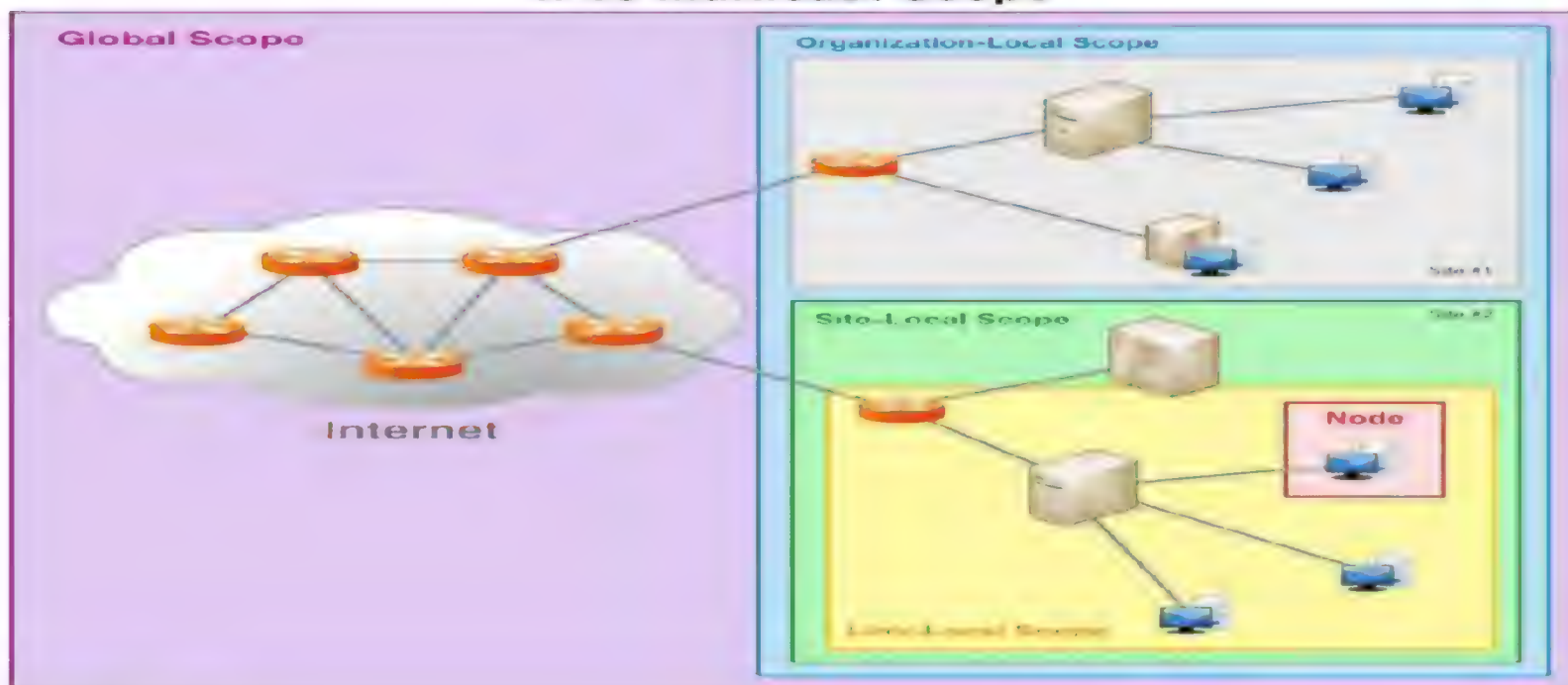
Where do IP addresses come from?

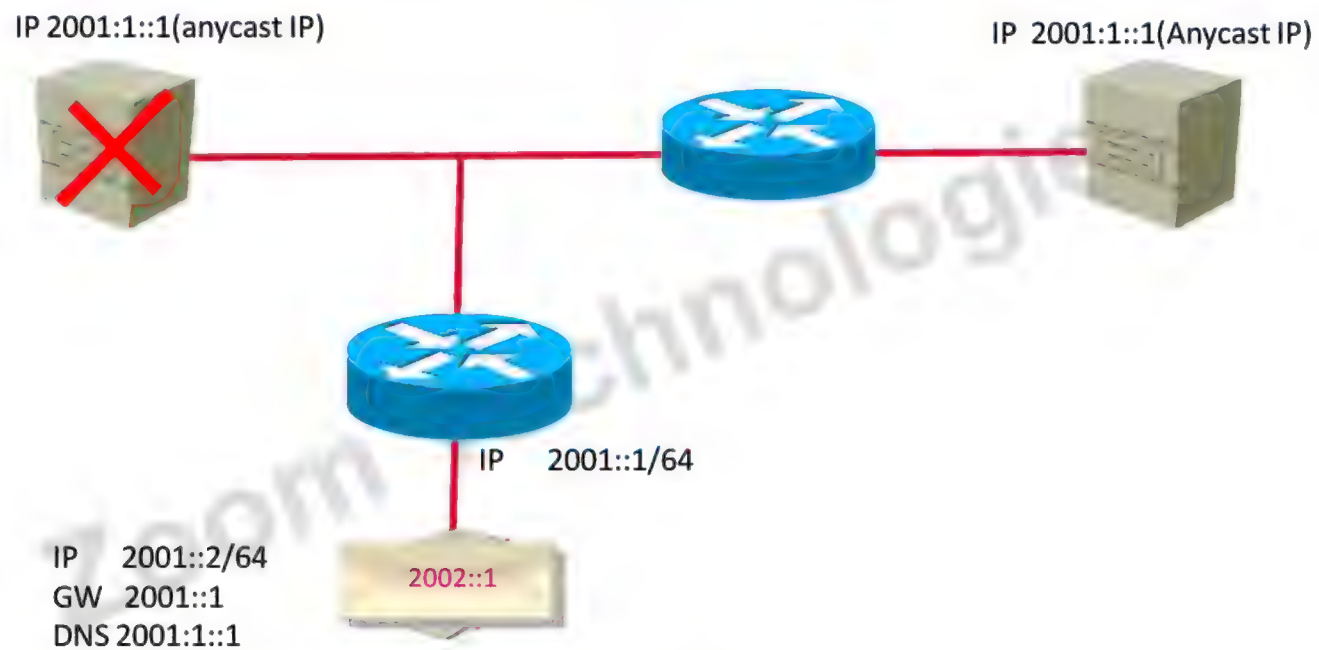


Multicasting



IPv6 Multicast Scope





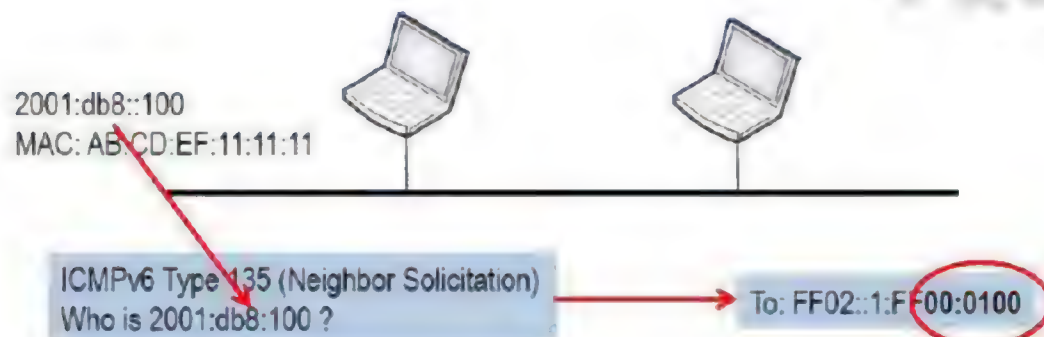
- One to nearest one
- Two or more devices share same anycast IP
- Nearest one will be decided by router by its routing protocol
- Anycast should give same type of service
- Anycast IP is used from Unicast range

Neighbor Discovery Protocol

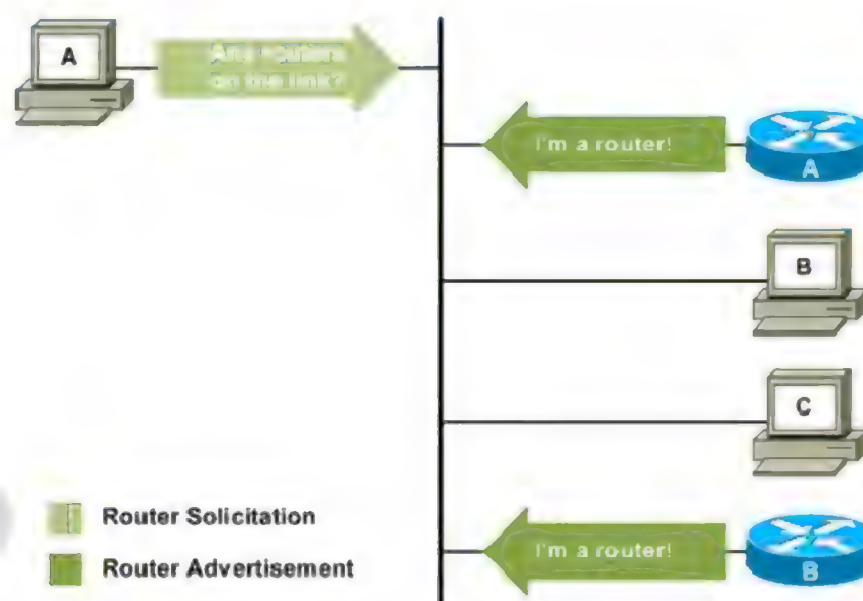
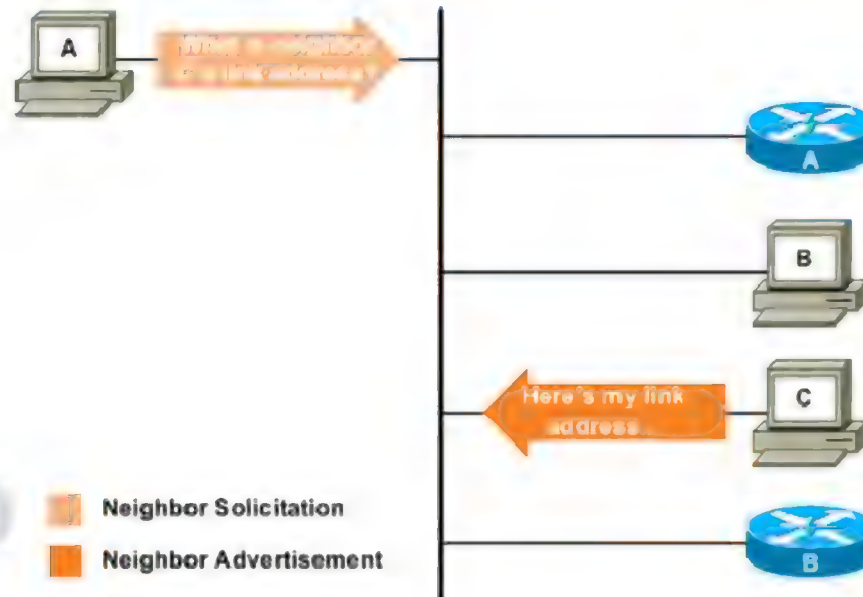
- Neighbor Discovery Protocol is Internet Protocol used in IPV6
- NDP uses 5 different messages for the operation
- NS(Neighbor Solicitation)
- NA(Neighbor Advertisement)
- RS(Router Solicitation)
- RA(Router Advertisement)
- Redirect

Zoom Technologies

DAD



20-



IPv6 Stateless Auto Configuration

- Device will assign IP address automatically by using stateless auto configuration.
- Extended universal identifier (EUI)-64 format to do stateless auto configuration
- This format expands the 48-bit MAC address to 64 bits by inserting “FFFE” into the middle of MAC address.
- 7th initial bit of MAC will be always “1”

EUI-64 To IPv6

00	90	27	17	FC	0F
----	----	----	----	----	----

02	90	27
----	----	----

FF	FE
----	----

17	FC	0F
----	----	----

0290:27FF:FE17:FC0F

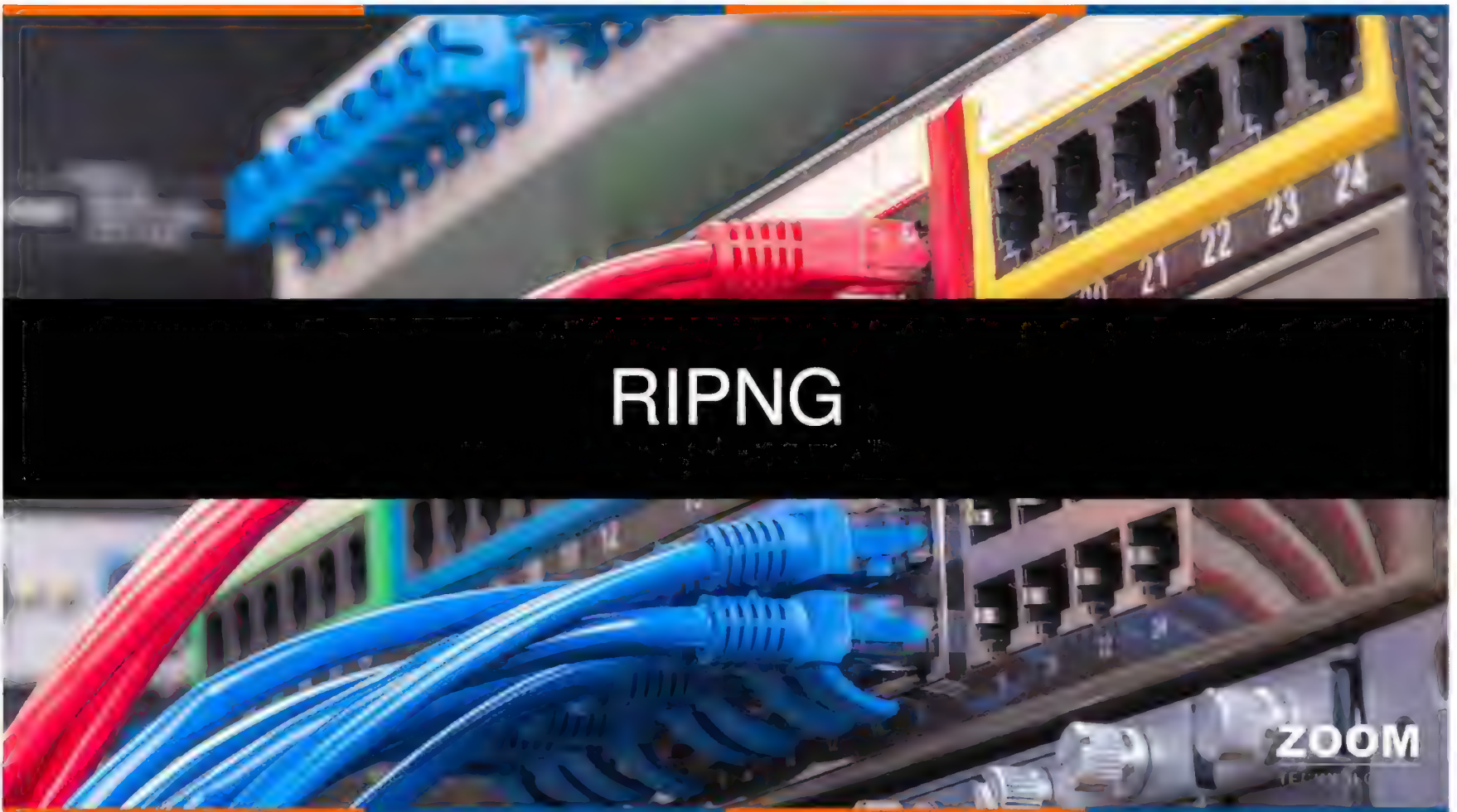
IPv6 Address	Description
:: /0	<ul style="list-style-type: none">• All routes and used when specifying a default static route.• It is equivalent to the IPv4 quad-zero (0.0.0.0).
:: /128	<ul style="list-style-type: none">• Unspecified address and is initially assigned to a host when it first resolves its local link address.
::1 /128	<ul style="list-style-type: none">• Loopback address of local host.• Equivalent to 127.0.0.1 in IPv4.
FE80 :: /10	<ul style="list-style-type: none">• Link-local unicast address.• Similar to the Windows autoconfiguration IP address of 169.254.x.x.
FF00 :: /8	<ul style="list-style-type: none">• Multicast addresses.
All other addresses	<ul style="list-style-type: none">• Global unicast address.



IPV6 Routing Protocols

- Static
- RIPng
- OSPFv3
- ISIS for IPv6
- EIGRP For IPv6
- MP BGP

Zoom Technologies



- RIP for IPv6
- Based on RIPv2, with enhancements
- Distributes IPv6 prefixes
- RIPng sends updates on UDP port 521 using the multicast group FF02::9.

Zoom Technologies

OSPF v3

- OSPF for IPv6
- Based on OSPFv2, with enhancements
- Distributes IPv6 prefixes
- Runs directly over IPv6
- Ships-in-the-night with OSPFv2



- Link-State Protocol
- SPF or Dijkstra algorithm
- Basic packet types
- Mechanisms for neighbor discovery and adjacency formation
- Same Interface types
- LSA flooding and aging mechanism
- OSPFv3 still uses Router ID from IPv4 Address



OSPF v2	OSPF v3
<ul style="list-style-type: none"> • Runs over subnet • One instance per link • Clear text or MD5 authentication • Router should be on the same subnet to form neighbors. • Uses Primary IP of outgoing interface as source of updates 	<ul style="list-style-type: none"> • Runs Over a Link • Multiple instance per link • Uses standard authentication supported by IPv6 I.E. IPSec • Router belonging to different subnet can become neighbor • Uses link local address as source of updates



- EIGRP for IPv6
- Uses Multicast address FF02::A
- EIGRPV6 remains in shutdown state until no shutdown is given.
- Manually need to configure Router-ID in EIGRPV6
- EIGRPV6 also uses DUAL algorithm

Zoom Technologies

IPV4 to IPV6

- **Transition Richness**
 - No Fixed day or time Due date for IPv4 to IPv6
 - Smooth transition from IPv4 to IPv6
 - Use Dual Stack or 6to4 tunnel
 - IPv4 to IPv6 host can communicate

Zoom Technologies

- A wide range of techniques have been identified and implemented, basically falling into three categories:
 - Dual-stack techniques, to allow IPv4 and IPv6 to co-exist in the same devices and networks
 - Tunneling techniques, to avoid order dependencies when upgrading hosts, routers, or regions
 - Translation techniques, to allow IPv6-only devices to communicate with IPv4-only devices.

Zoom Technologies

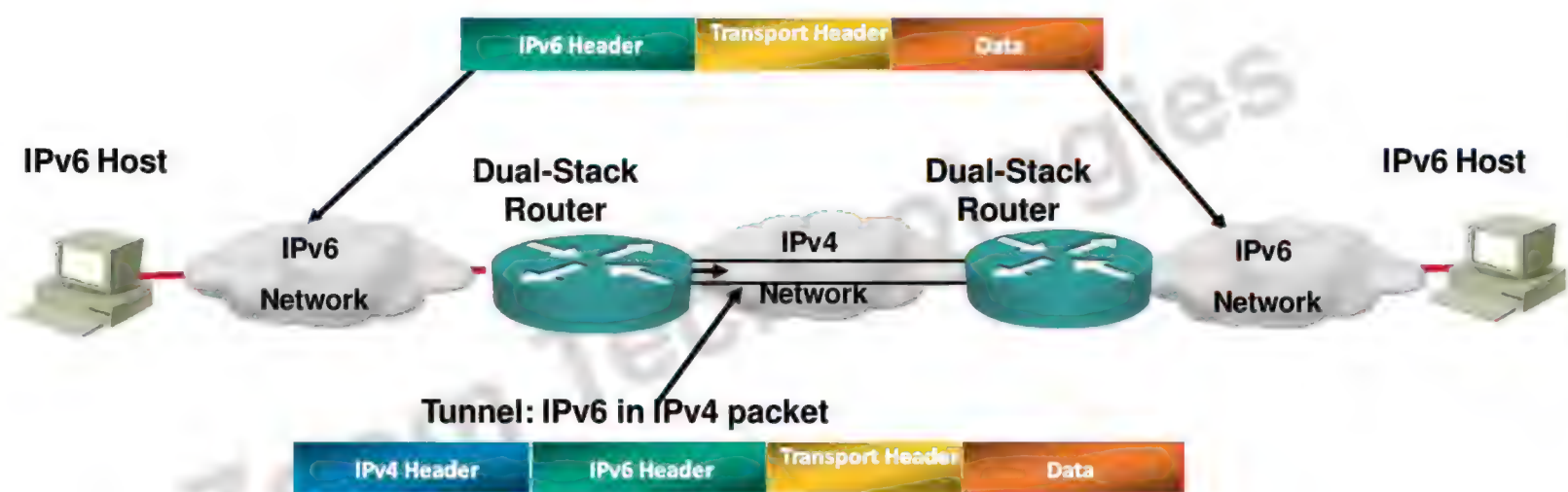
DUAL Stack

- The term dual stacks means that the host or router uses both IPv4 and IPv6 at the same time.

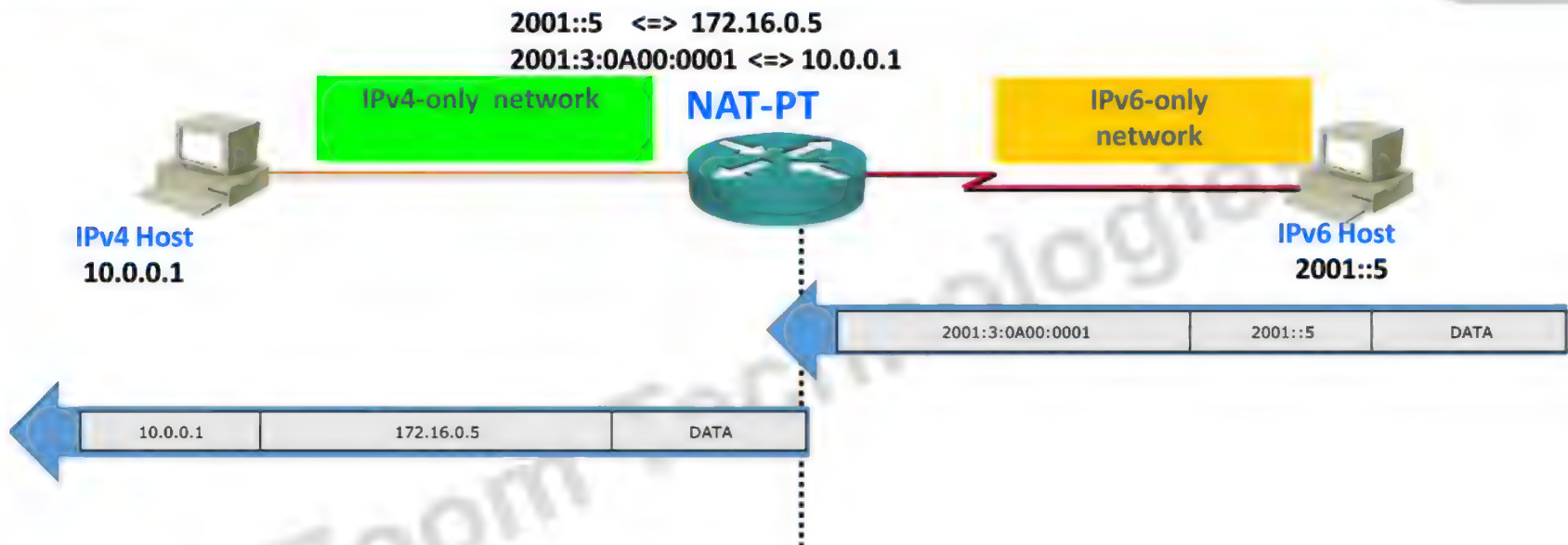


- Cisco IOS is IPv6-enabled:
 - If IPv4 and IPv6 are configured on one interface, the router is dual-stacked

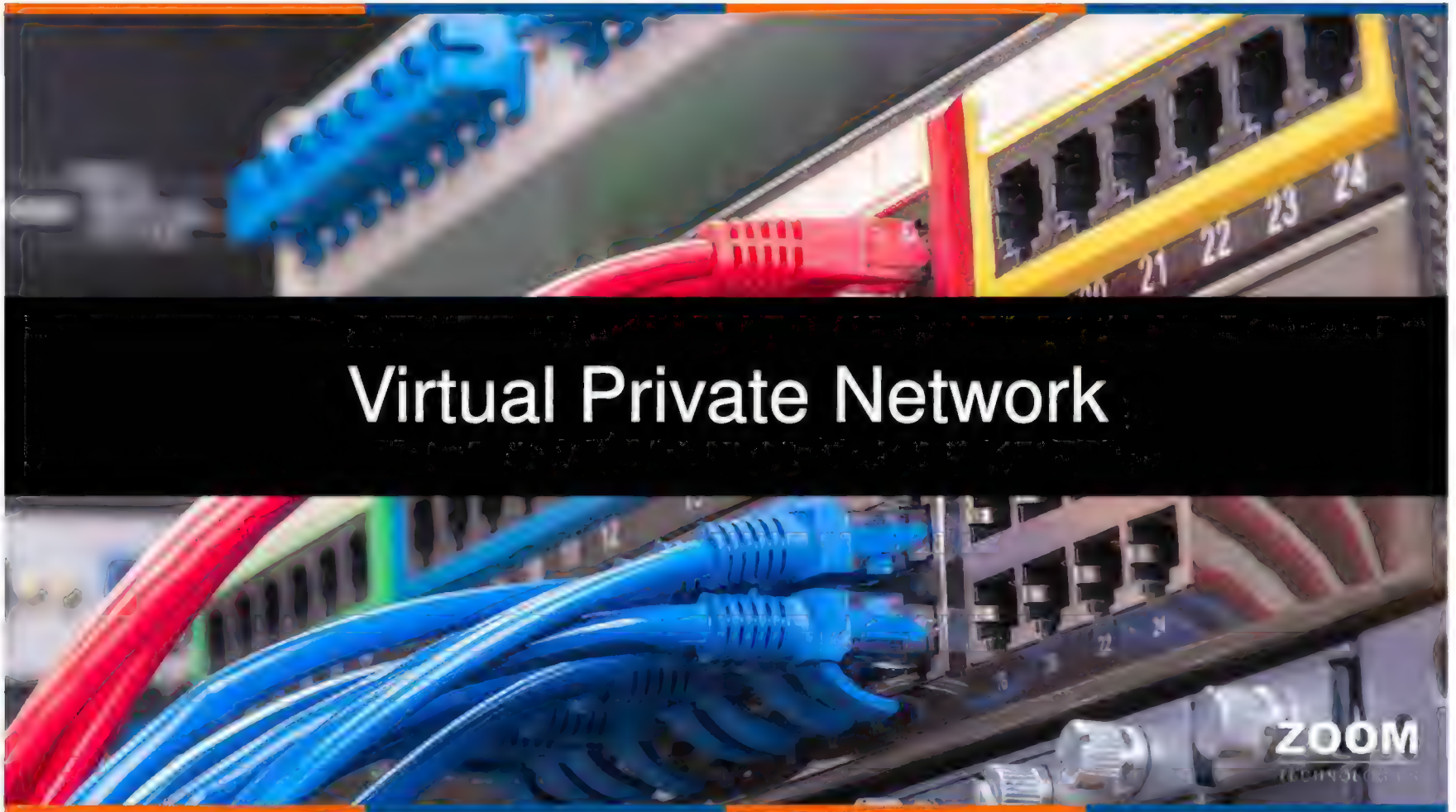
IPv6 over IPv4 Tunnels



- Tunneling is encapsulating the IPv6 packet in the IPv4 packet
- Tunneling can be used by routers and hosts



- ISATAP- Intra-Site Automatic Tunnel Addressing Protocol
- ISATAP is a method of automatic 6 to 4 Tunnels.
- ISATAP is a mechanism that allows us to deploy IPv6 over existing IPv4 infrastructure.
- ISATAP connects two regions of IPv6 via a tunnel that will transit over existing IPv4 infrastructure.



Virtual Private Networking

ZOOM
TECHNOLOGIES

- Virtual Network → Tunneling



- Private Network → Encryption



- Virtual Private Network = Tunneling + Encryption

013G_353



- **Services Offered by VPN are:**

- Data Security
- Data Integrity
- Authentication
- Anti-Replay
- Tunneling

Devices Supports VPN

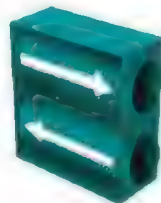
Routers



Firewall



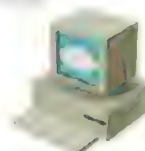
VPN concentrator



Servers



Cisco VPN Client v 5



- **Remote-access**

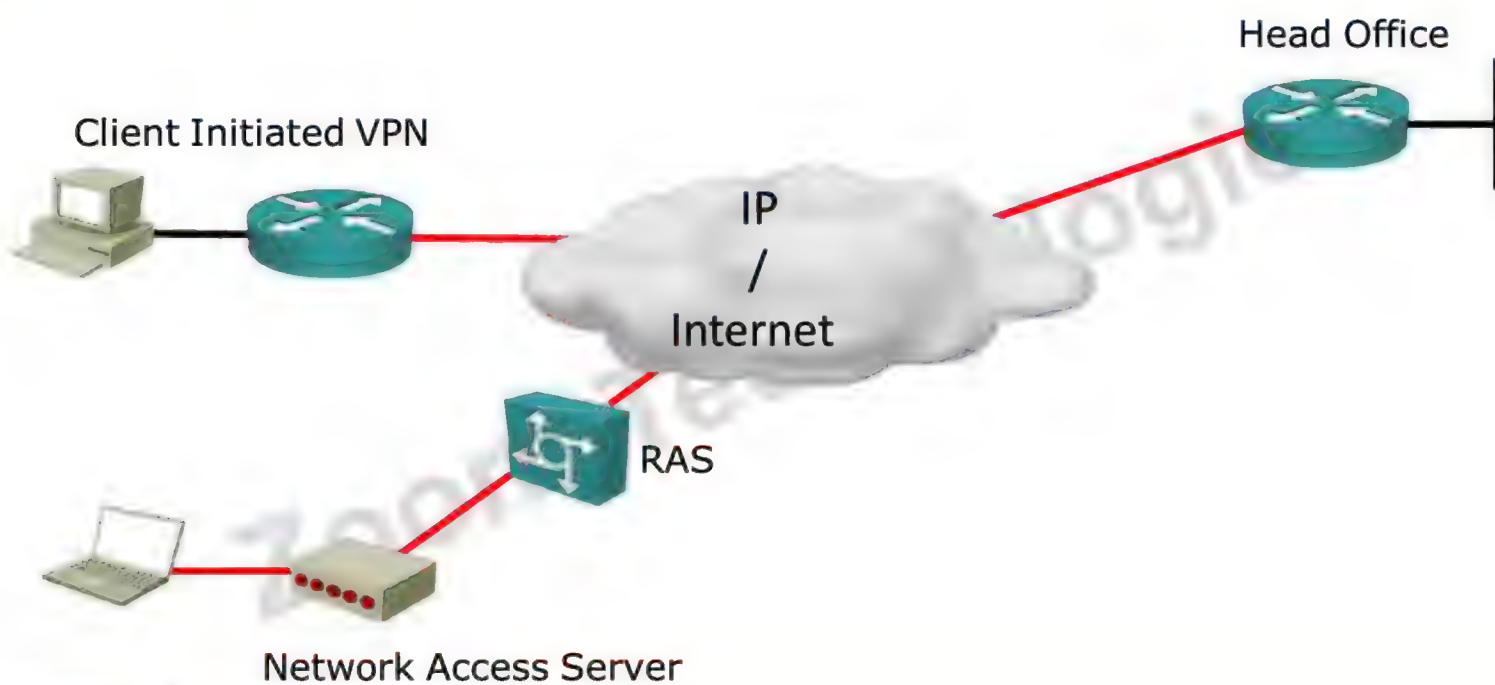
- Client-initiated
- Network access server

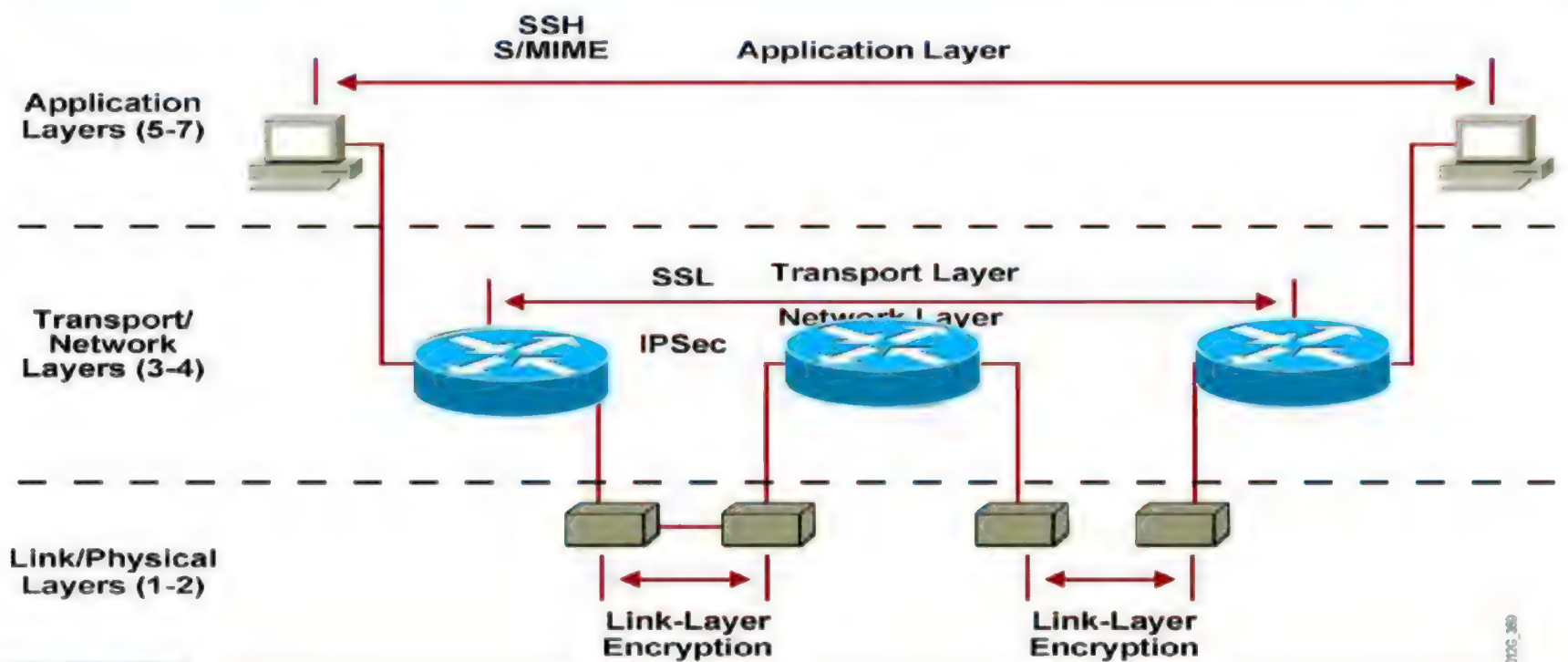
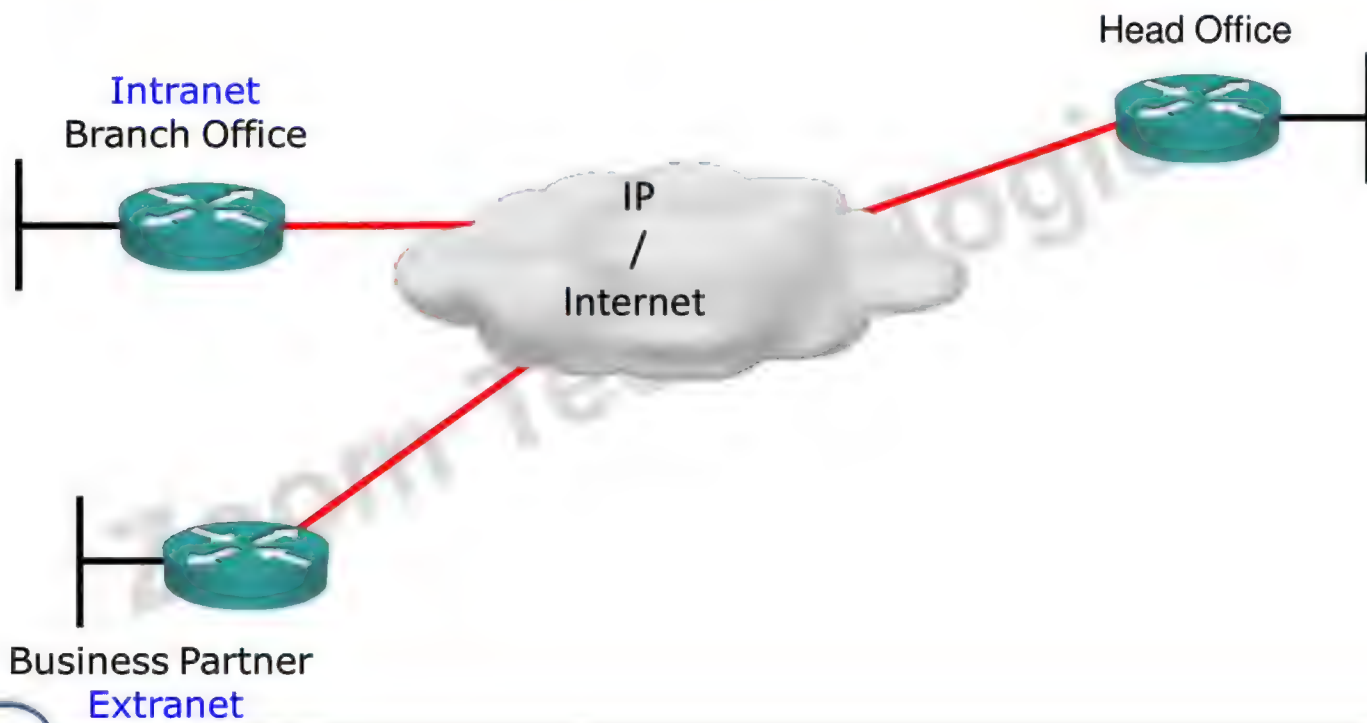
- **Site-to-site**

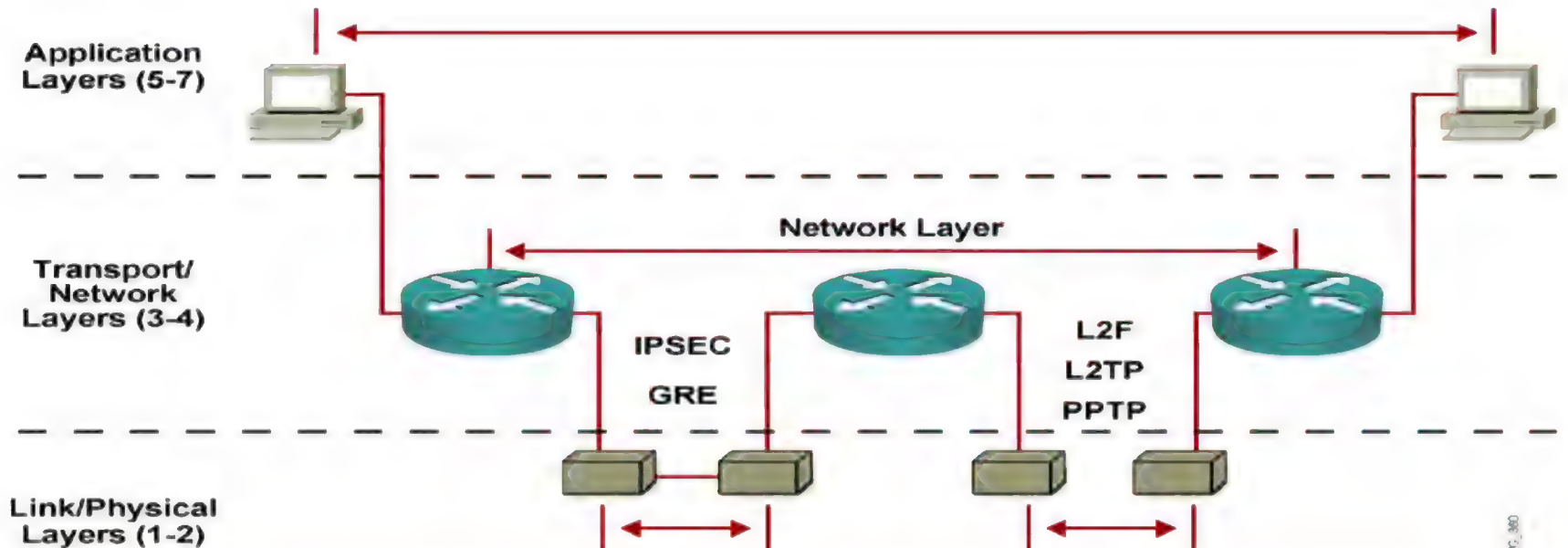
- Intranet
- Extranet



Remote Access VPN



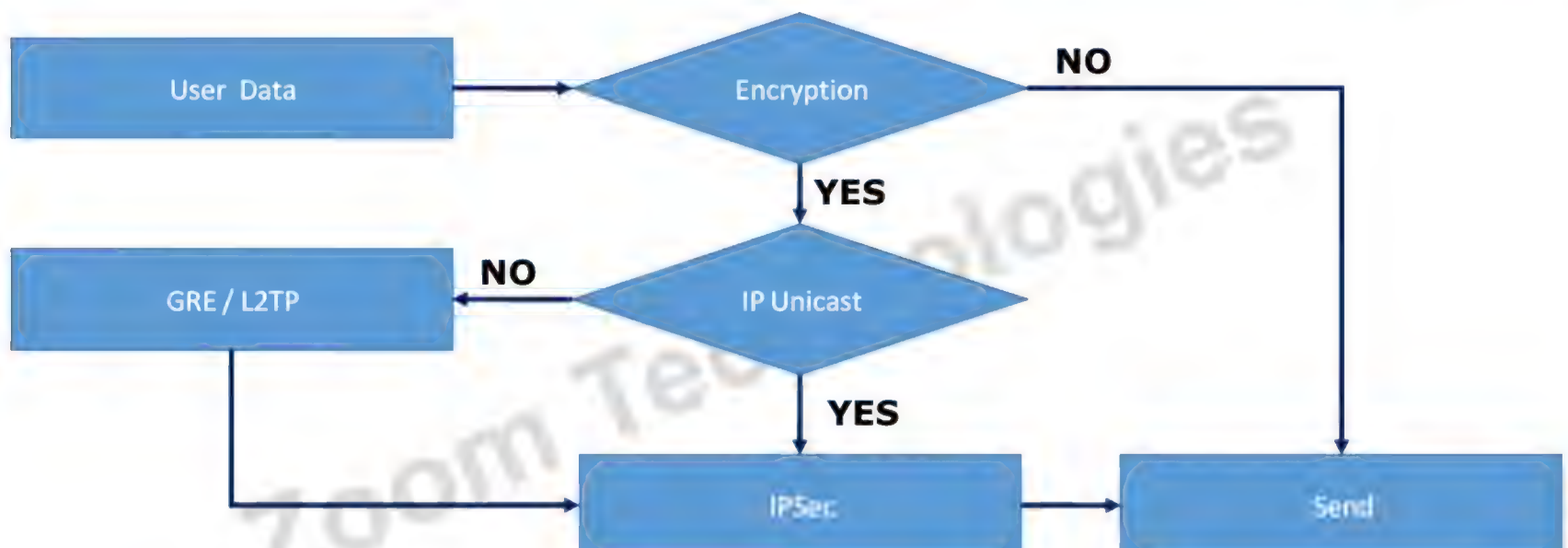




Generic Routing Protocol



- IPSec is a open standard (IETF)
- Network layer protocol
- It provides Data security and tunneling services
- It is a framework consisting of many open standards providing encryption , authentication, key exchange and data integrity.
- Scales from small to very large networks
- It can Work only for IP unicast traffic
- IPSec over GRE is used for protecting non-IP or Multicast traffic



- **IPSec modes:**

- Tunnel Mode
 - Tunnel mode creates a new additional IP header with data encryption
- Transport mode
 - just encrypt data without adding new IP header



IPSEC PROTOCOLS

- **Negotiation protocol**
 - IKE /ISAKMP
- **Security Protocol**
 - ESP
 - AH



- **Encryption**
 - DES
 - 3DES
 - AES
- **Hash**
 - MD5
 - SHA
- **Authentication**
 - Pre-share key
 - Username/Password
 - OTP
- **Password Protection** (Diffie-Hellman for password exchange)
 - DH Group 1
 - DH Group 2
 - DH Group 5



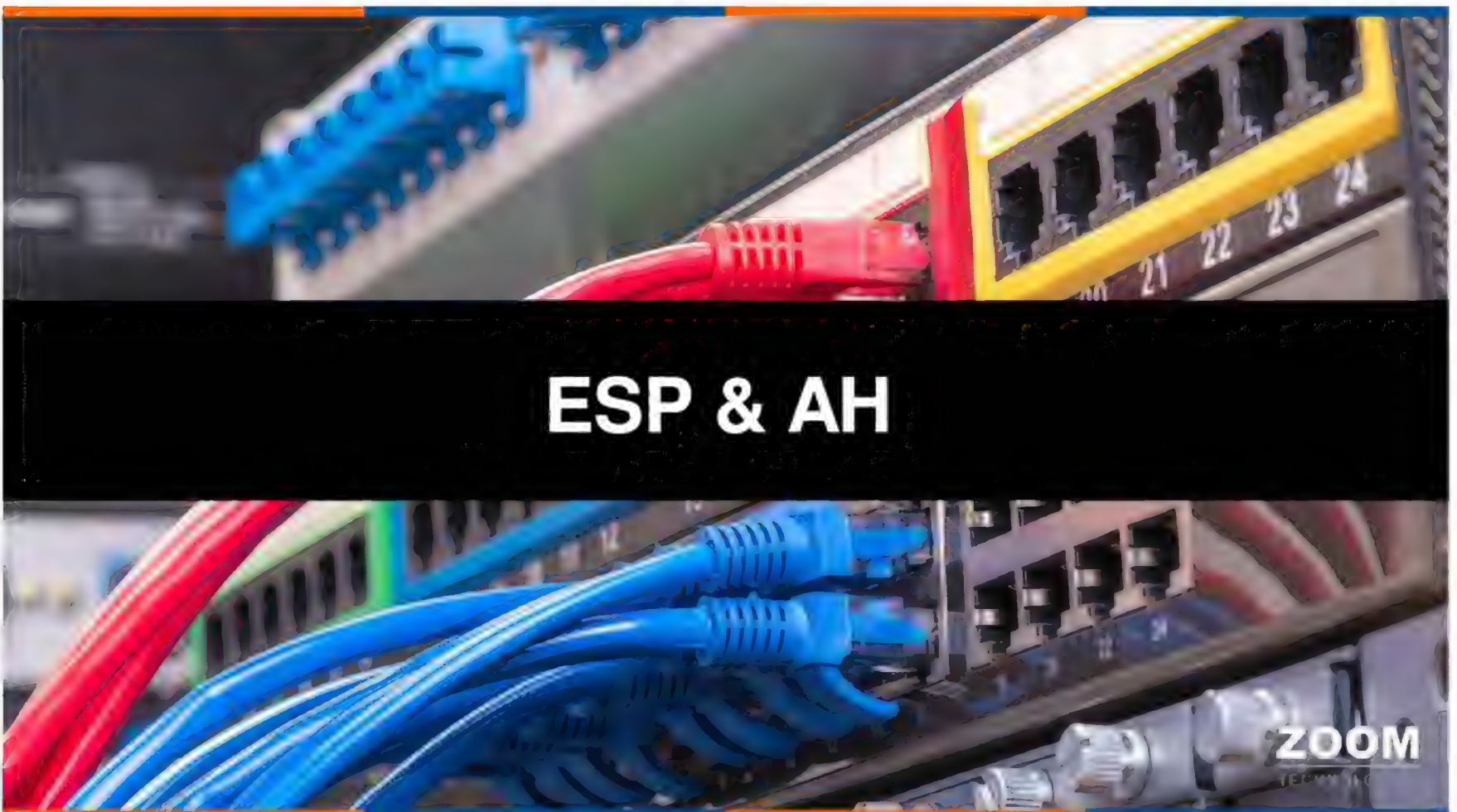
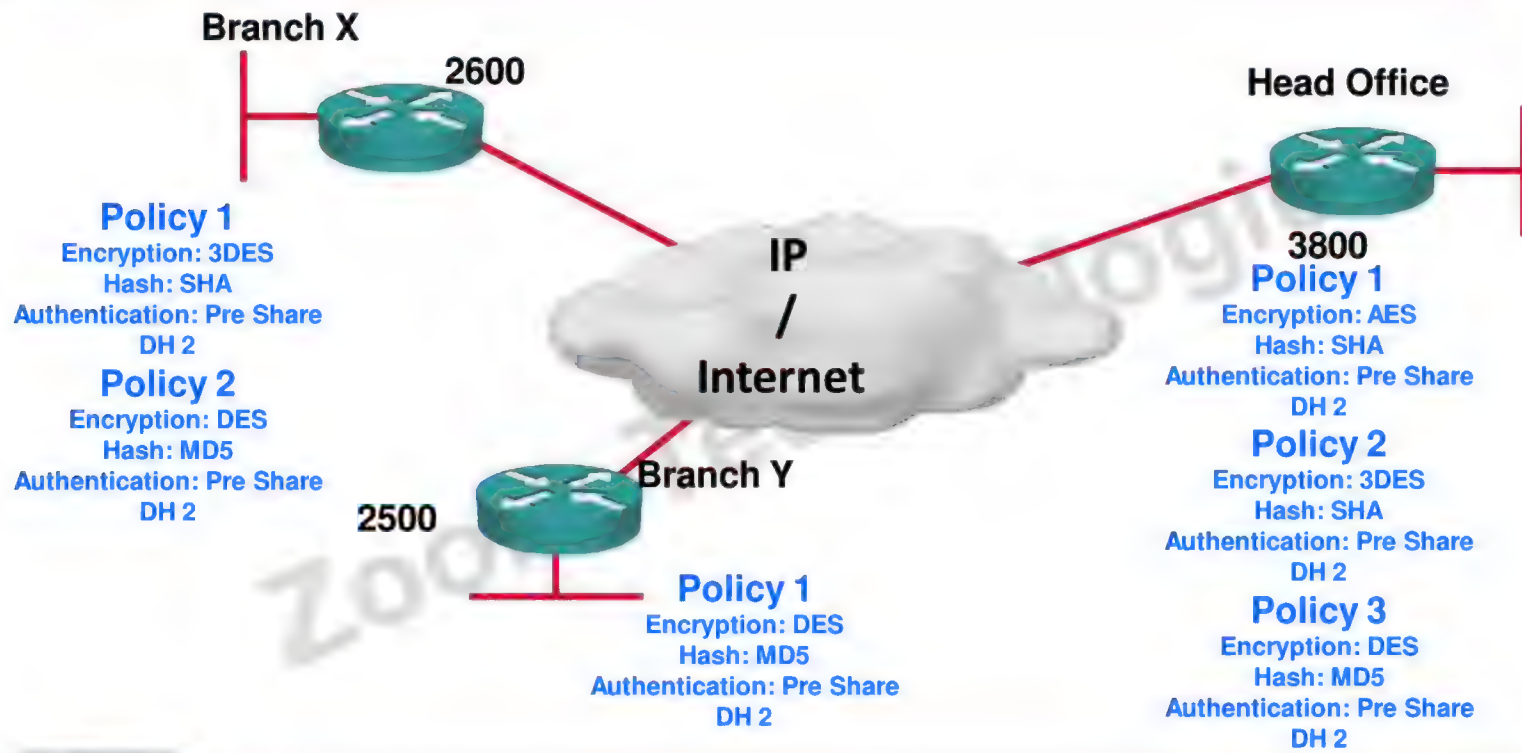


Internet Key Exchange

ZOOM
TECHNOLOGIES

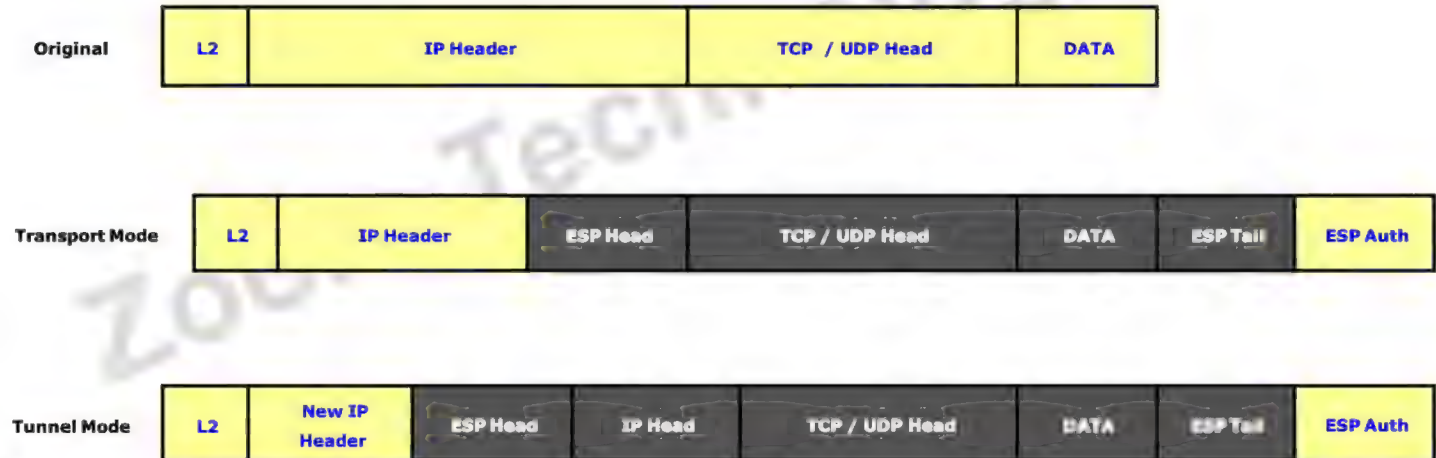
- IKE solves the problems of manual and unsalable implementation of IPSec by automating the Negotiation Process
 - Automatic key generation, negotiation and implementation
 - Negotiation of SA characteristics
 - Manageable manual configuration





Encapsulating Security Payload

- ESP protocol ID 50
- Provides framework for encrypting, authenticating and data integrity. Optional Anti-replay



Authentication Header

- AH protocol ID 51
- Provides framework for authenticating and data integrity. Optional Anti-Replay



DMVPN

ZOOM
TECHNOLOGIES

- DMVPN allows a vpn tunnel to dynamically created and torn down between two remote sites.
- DMVPN uses NHRP and multipoint GRE to perform this operation.

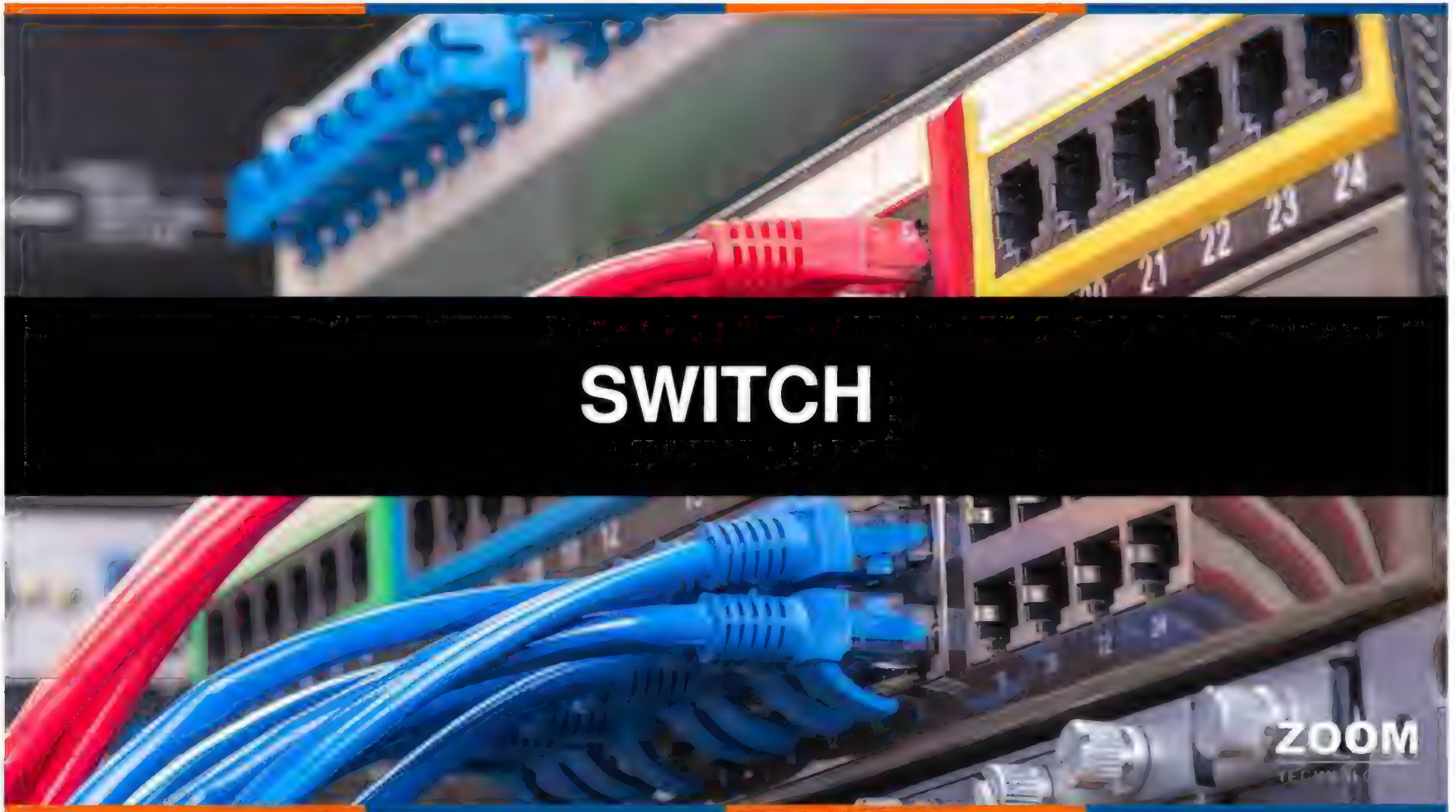
Zoom Technologies

CCIE
CCNP
CCNA

ZOOM
TECHNOLOGIES

Zoom Technologies

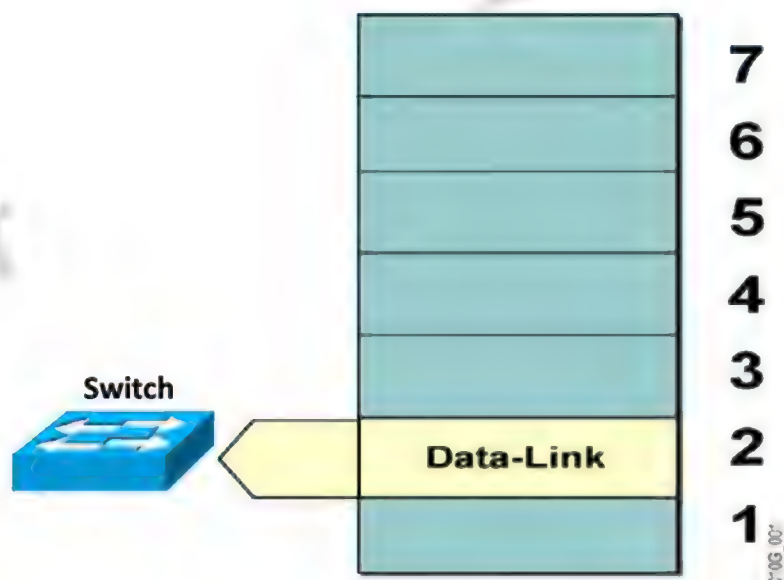
CCIE
CCNP
CCNA



Layer 2 Switching

ZOOM
TECHNOLOGIES

- Hardware-based bridging
- Wire-speed performance
- High-speed scalability
- Low latency
- Uses MAC address



- Hardware-based packet forwarding
- High-performance packet switching
- Flow accounting
- Layer 3 security
- Policy deployment

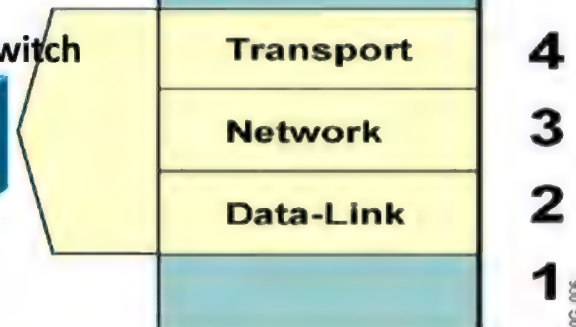
Layer 3 switch



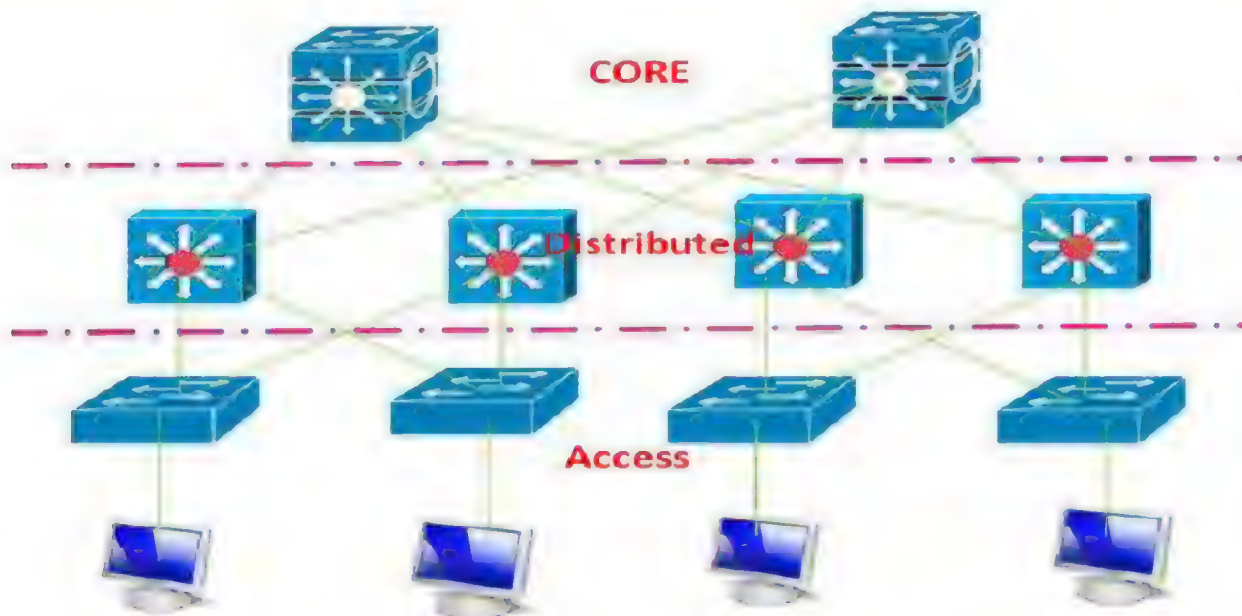
010G_004

- Combines functionality of:
 - Layer 2 switching
 - Layer 3 switching
 - Layer 4 switching
- High-speed scalability
- Low latency

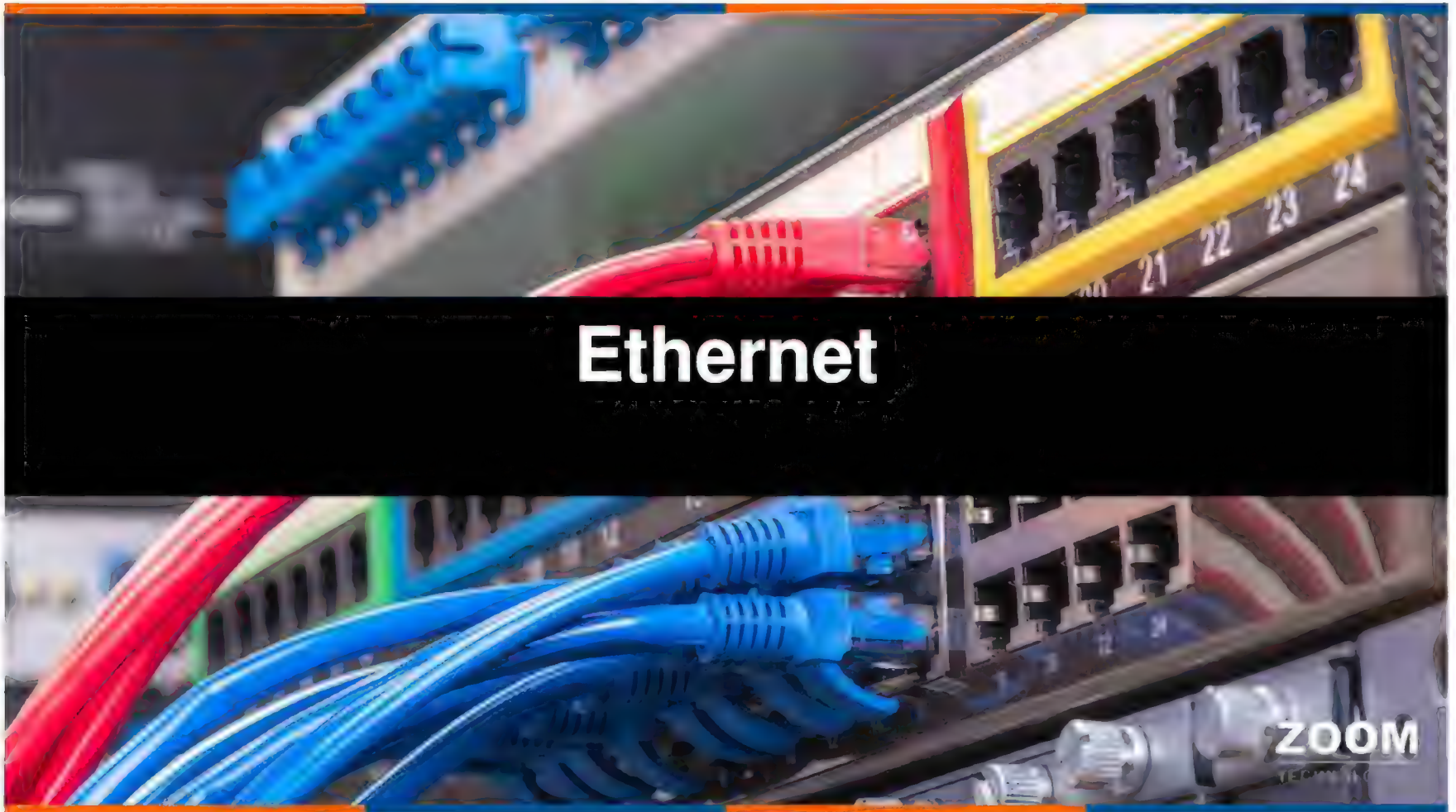
Multi layer switch



010G_006

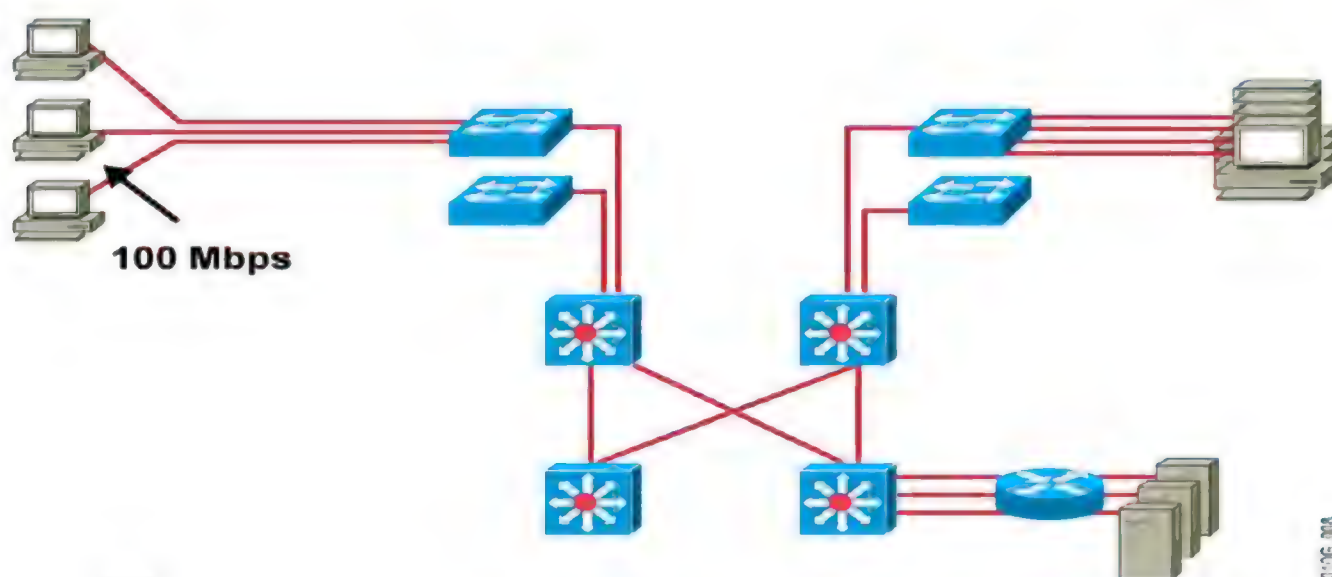


- **Access Layer:**
 - Access Layer switches are used to connect end devices to the network
 - Access Layer Switches used to provide Layer2 (VLAN) connectivity between users.
 - Ex: 2950,2960 switches
- **Distribution Layer:**
 - Distribution Layer switches are used to interconnect access layer switches to core layer switches.
 - Distribution Layer is a Layer 3 Boundary where routing meets the VLANs of access layer switches.
 - Ex: 3550,3560,3750,4500 Switches
- **Core Layer**
 - Core Layer provides interconnectivity between all distribution layer switches.
 - Core Layer is sometimes also called as Backbone must be capable of forwarding traffic from one distribution layer to other distribution layer switch as efficiently as possible
 - Ex: 6500 Switch



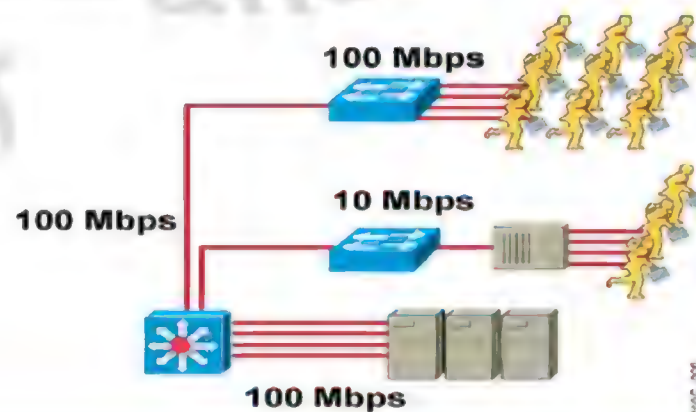
Fast Ethernet

ZOOM
TECHNOLOGIES

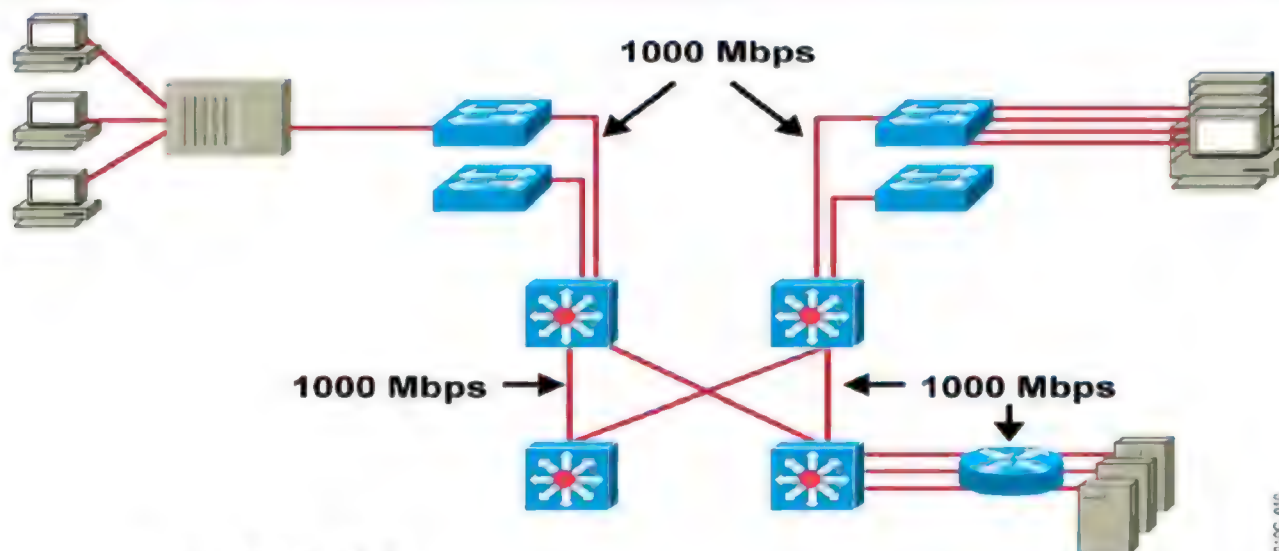


- Provides client access to the network

- Built on Ethernet principles
- Bandwidth - 100 Mbps
- Uses same frame types, lengths, and formats
- Still CSMA/CD
- Same MAC layer, new physical layer

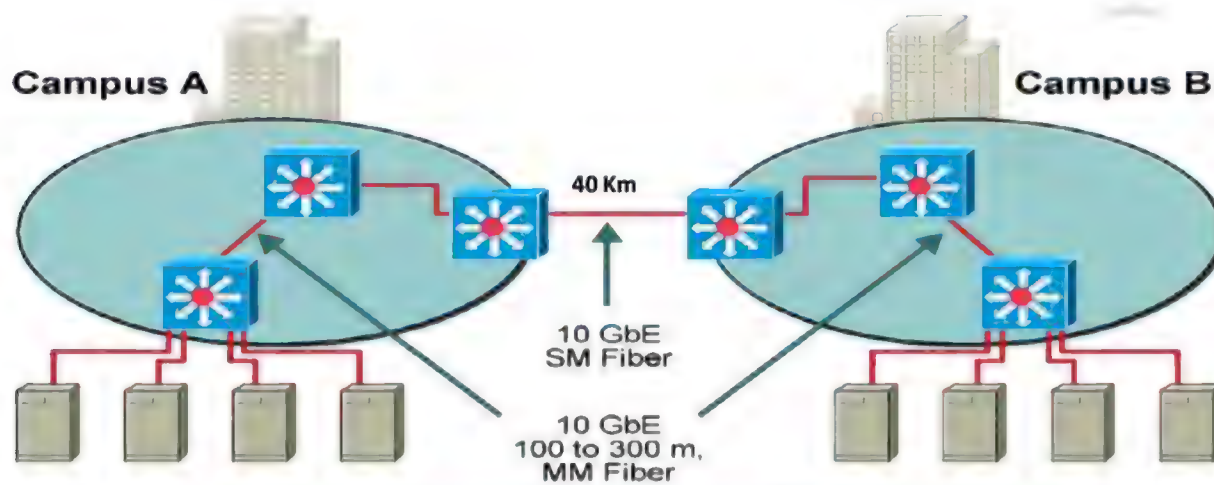


0105_008



0105_010

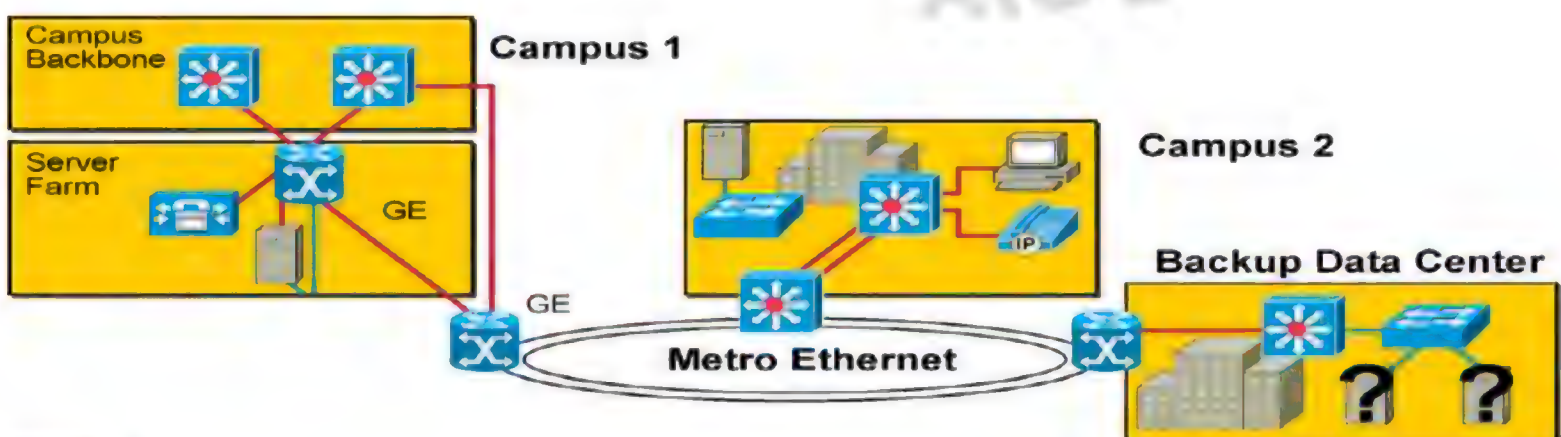
- Enhances client/server performance across the enterprise
- Connects distribution-layer switches in each building with a central campus core



- Cost-effective bandwidth for the LAN, switch-to-switch
- Used to aggregate multiple Gigabit Ethernet segments
- 10 Gigabit EtherChannel will enable 20 to 80 Gbps (future)

0105_011

- Leverages service provider network or existing, unused optical fiber (dark fiber) for metro Ethernet connectivity
- Supports any IP application



0103_012

- Store and Forward
- Cut Through
- Fragment Free



FCS	L3, L4, and Data	Ether Type	Source MAC	Dest. MAC
-----	------------------	------------	------------	-----------



In Store and Forward switching, Switch copies each complete frame into the switch memory and performs CRC(cyclic Redundancy Check) on that frame. If there are any errors it will drop that frame, if there are no errors it will forward the frame.

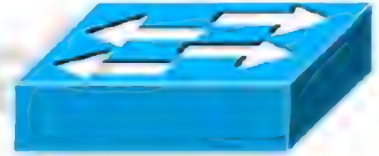
Delay is high , number of frames forwarded is low when compared to other types of switching



Cut Through

ZOOM
TECHNOLOGIES

FCS	L3, L4, and Data	Ether Type	Source MAC	Dest. MAC
-----	------------------	------------	------------	-----------



In cut-through switching, the switch copies only the destination MAC address (first 6 bytes of the frame) of the frame into its memory before making a switching decision.

More Errors - because it is not performing CRC.

Low Delay



Fragment Free

ZOOM
TECHNOLOGIES

FCS	L3, L4, and Data	Ether Type	Source MAC	Dest. MAC
-----	------------------	------------	------------	-----------



Fragment-free (runtless switching) switching is an advanced form of cut-through switching. The switches operating in fragment-free switching read at least 64 bytes of the Ethernet frame before switching it to avoid forwarding Ethernet runt frames (Ethernet frames smaller than 64 bytes).





Getting Started with Cisco Catalyst Switches

Cat OS and Cisco IOS (Native Mode)

ZOOM
TECHNOLOGIES

- Cat OS
 - Layer 2 switching functions
- Hybrid Mode
 - Cat OS for Layer 2 switching
 - IOS for Layer 3
- Cisco IOS (Native Mode)
 - Works for both Layer 2/Layer 3 switching
 - Runs on a device that can have a port that acts like a router port (Layer 3) or like a switched port (Layer 2)
 - Available on all new Catalyst switches



CAM Table

CAM Table is used to store layer 2 information like

- Source MAC address
- Interface where we learned the source MAC address
- Vlan information

TCAM Table

TCAM table is used to store higher information like

- Access-list
- QOS
- Routing Table

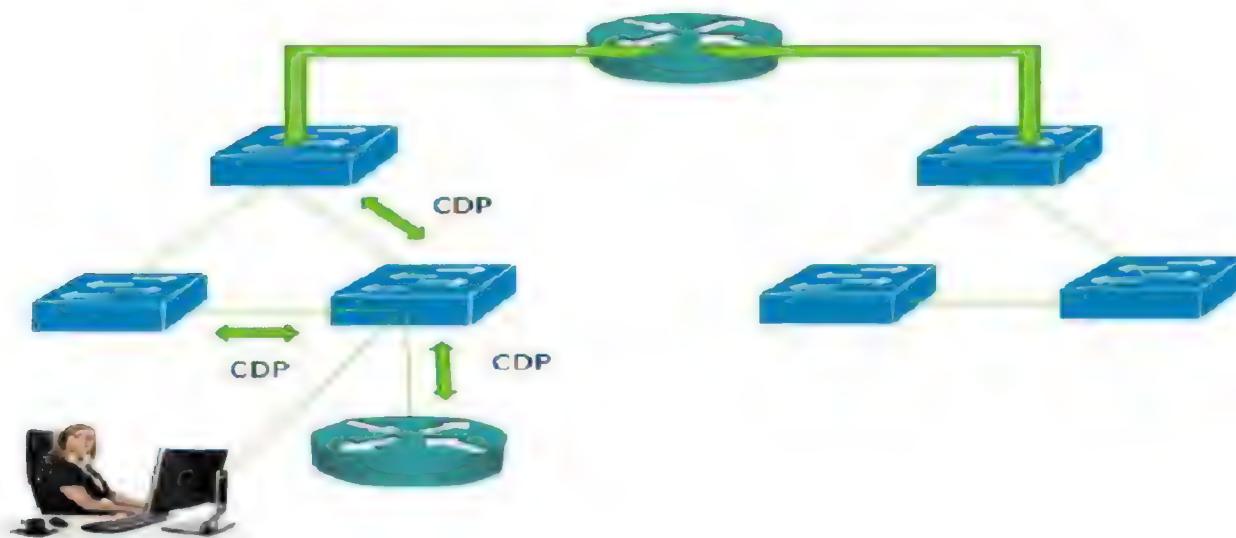


- CDP is a Layer 2 protocol used to find information about neighbor devices
- CDP Advertisements are sent as multicast frames.
- By default CDP is enabled on all Cisco devices.
- If an attacker is listening to CDP messages, it could learn important information about the device model and the current software version

Note: Cisco recommends disabling CDP when not in use.



- To get the information about neighbors by using CDP
`#show cdp neighbors`



- LLDP is similar to CDP but works on multi vendor networks.
- LLDP is an IEEE 802.1AB standard
- By default LLDP is disabled on Cisco devices.
- To enable LLDP on a Cisco device

Switch(conf)#lldp run



Virtual LANs

ZOOM
TECHNOLOGIES

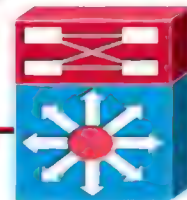
- VLANs are used to divide one large broadcast domain into multiple smaller broadcast domains.
- A large network can be divided into VLANs based on Project, Department or function etc.
- VLANs provide Broadcast Segmentation
- Each VLAN is a single Broadcast domain



Static



Dynamic

Switch
5500

Static VLANS

- Static Vlan are also called as port-based vlans.
- Any device connecting to the port will become a member of that Vlan.
- This is the most common method of assigning ports to VLANs
- There is a default VLAN, on Cisco switches :VLAN 1

Dynamic Vlan



- Dynamic Vlans are also called MAC based vlans.
- Vlans are automatically created by switch and assigned as per the mac address of the connected device.
- Dynamic vlans are flexible compared to static vlans.
- VMPS is required to configure Dynamic Vlans.



Voice Vlan



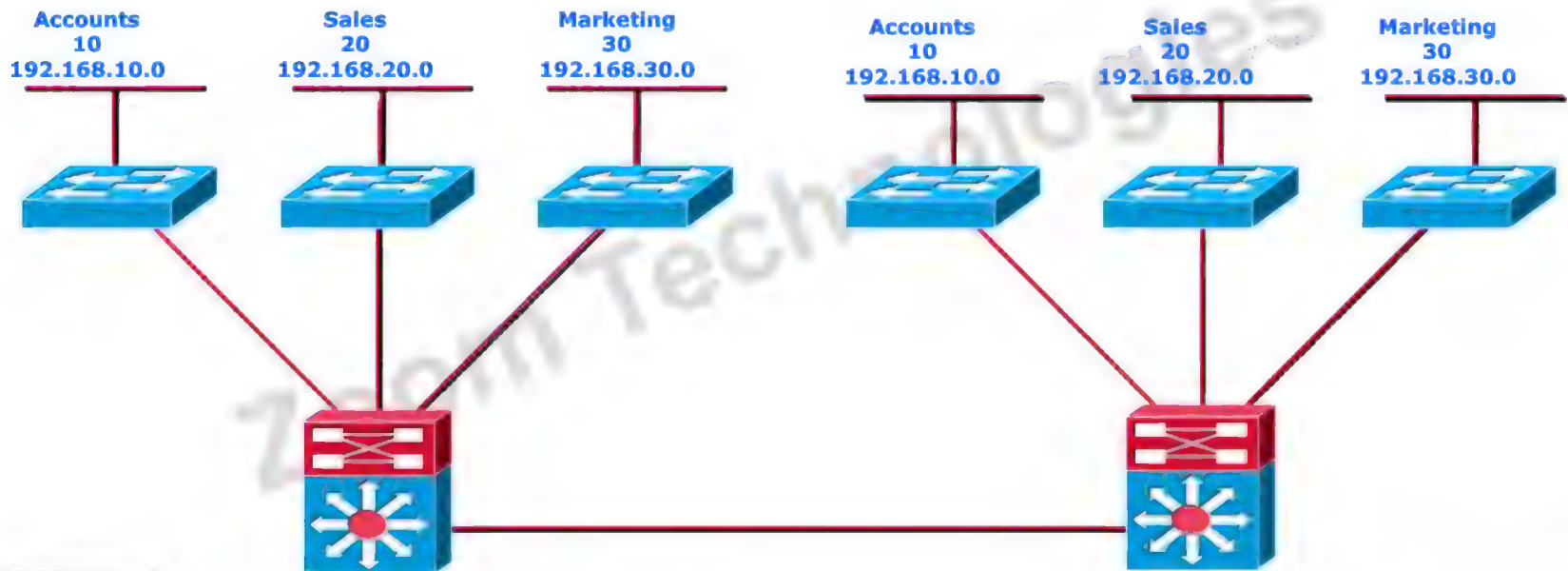
- Voice Vlan allows access ports to carry voice traffic from an IP phone
- By default voice vlan feature is disabled.
- To enable, Give the following command

Switch(conf-if)# switchport voice vlan 10



End to End Vlan

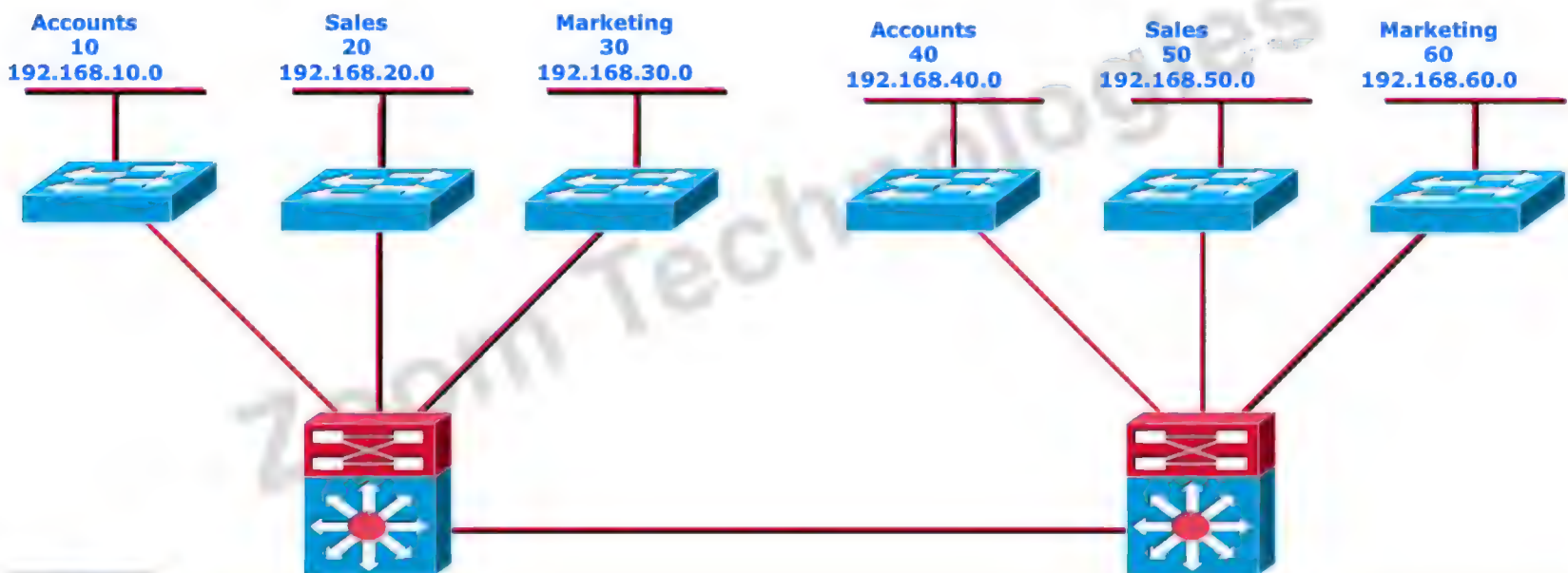
ZOOM
TECHNOLOGIES



CCIE
CCNP
CCNA

Local Vlan

ZOOM
TECHNOLOGIES



CCIE
CCNP
CCNA

VLAN Range	Range	Usage
1	Normal	Cisco default
2-1001	Normal	For Ethernet VLANs
1002-1005	Normal	Cisco defaults for FDDI and Token Ring
1006-4094	Extended	For Ethernet VLANs

```
Switch(config)#Vlan <no>
```

```
Switch(config-vlan)#name <name>
```

Assigning Access Ports to a VLAN

```
Switch(config)#interface gigabitethernet 1/1
```

- Enters interface configuration mode

```
Switch(config-if)#switchport mode access
```

- Configures the interface as an access port

```
Switch(config-if)#switchport access vlan 3
```

- Assigns the access port to a VLAN



Verifying VLANs – show vlan



```
SydneySwitch#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4
2	VLAN2	active	Fa0/5, Fa0/6, Fa0/7
3	VLAN3	active	Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	1002	1003
2	enet	100002	1500	-	-	-	-	-	0	0



```
S1# conf t
S1(config)# no vlan 20
S1(config)# end
S1#
S1# sh vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gi0/1 Gi0/2
1002	fdi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fdiinet-default	act/unsup	
1005	trnet-default	act/unsup	

```
S1#
```

Switch(config-if)#no switchport access vlan vlan_number

- This command will reset the interface to VLAN 1.
- VLAN 1 cannot be removed from the switch.



Implementing VLAN Trunks

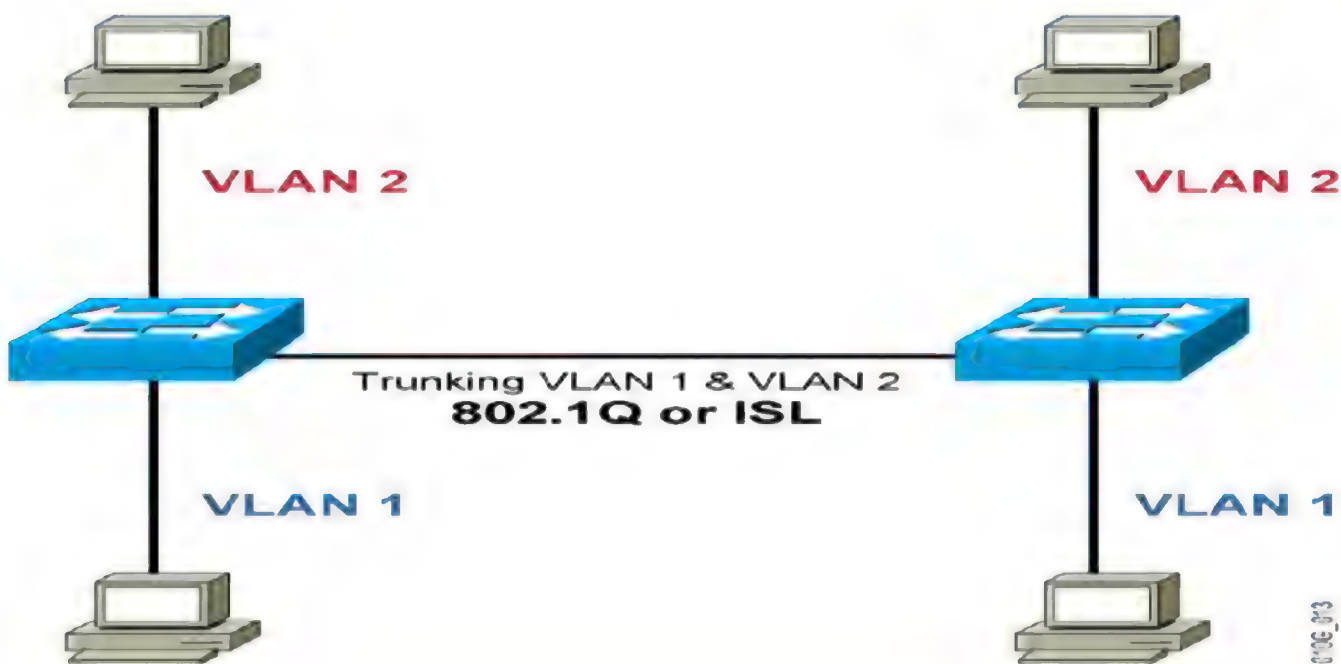


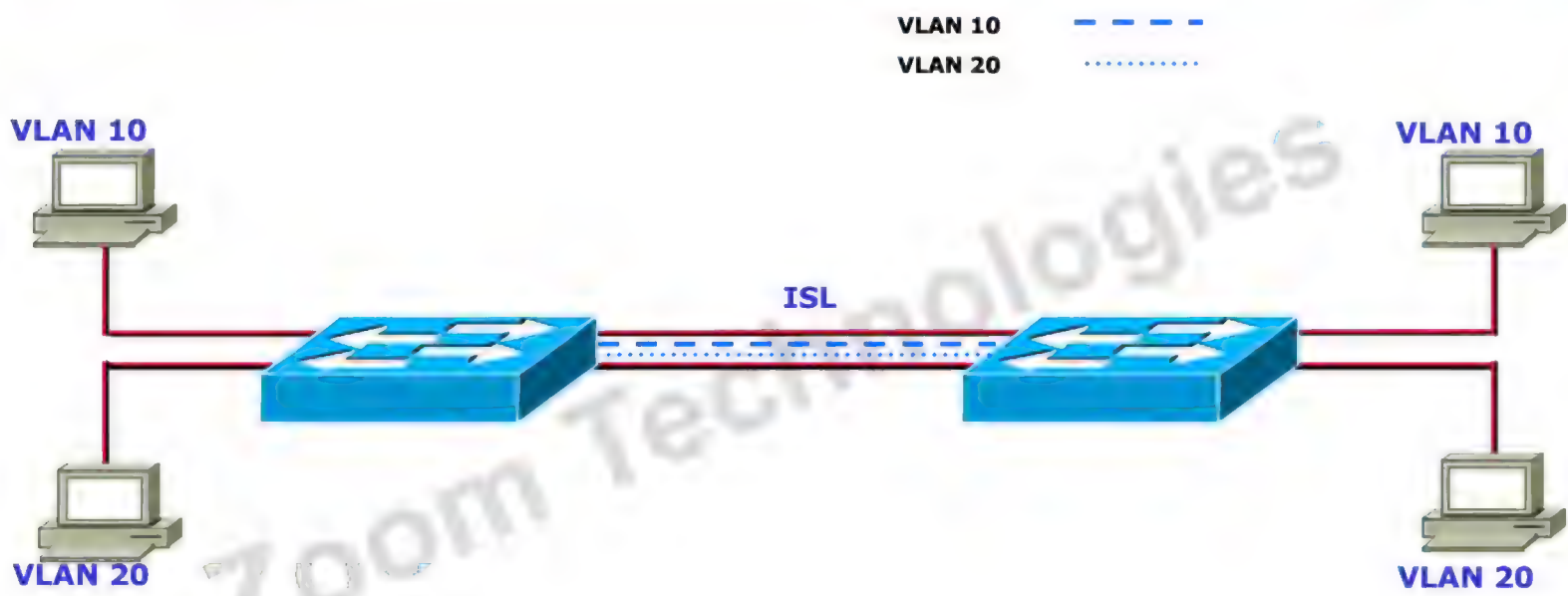
Trunking Encapsulation

- VLANs are local to each switch's database, and VLAN information is not passed between switches. Trunks carry traffic from all VLANs to and from the switch by default but can be configured to carry only specified VLAN traffic.
- Two types of trunking encapsulation protocols
- ISL(Inter Switch Link)
- 802.1Q(Dot 1Q)

Zoom Technologies

VLAN Trunk Encapsulation





ISL Encapsulated Layer 2 Frame from an ISL Trunk Port

ISL Header (26B)	DA (6B)	SA (6B)	Length/ Etype (2B)	Data (0-1500 Bytes)	FCS (4B)	ISL FCS (4B)
---------------------	------------	------------	--------------------------	------------------------	-------------	--------------------

Untagged and Unencapsulated Layer 2 Frame from an Access Port

DA (6B)	SA (6B)	Len/Etype (2B)	Data (0-1500B)	FCS (4B)
------------	------------	-------------------	-------------------	-------------

010G_016



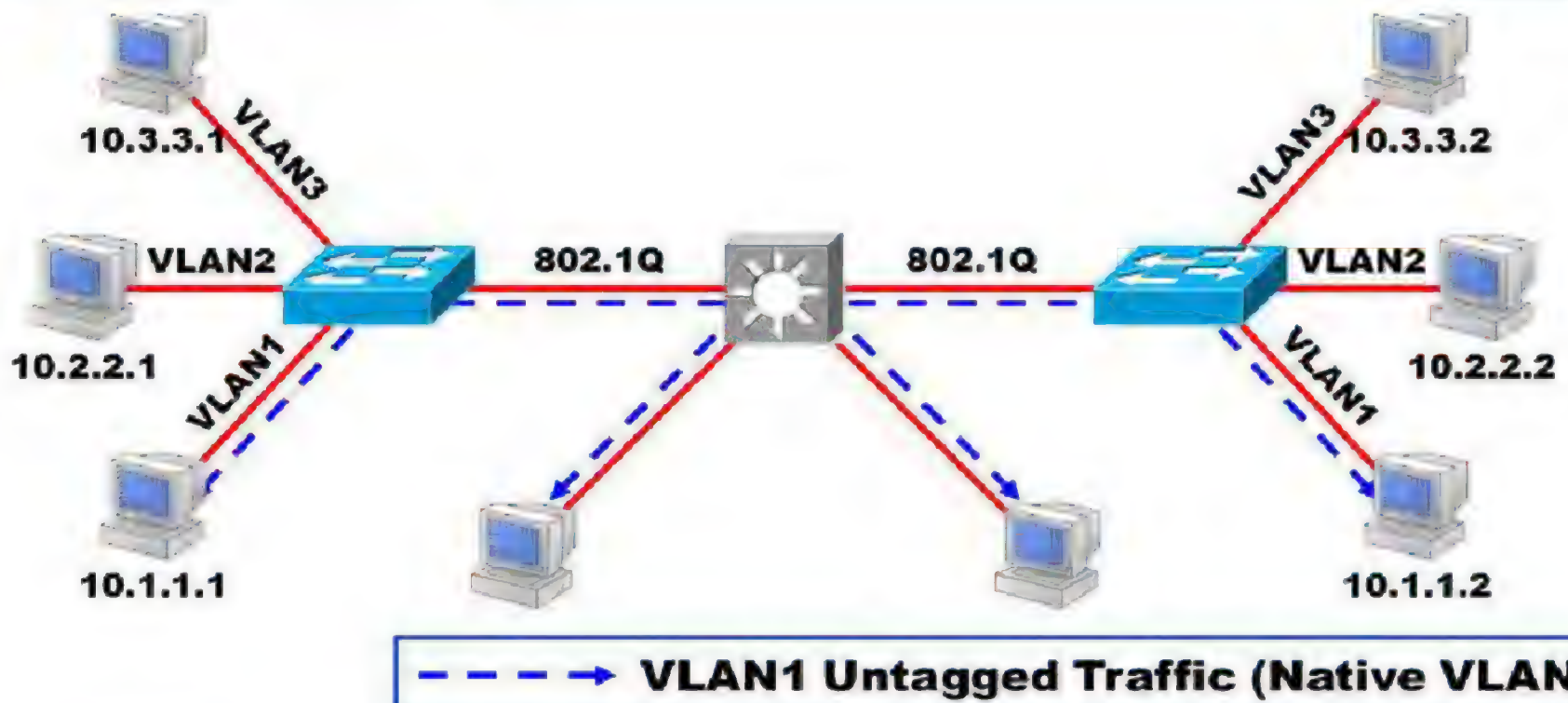
802.1Q Tagged Layer 2 Frame from an 802.1Q Trunk Port

DA (6B)	SA (6B)	Etype (8100) (2B)	Dot1Q Trunk Tag (2B)	Length/ Etype (2B)	Data (0-1500 Bytes)	FCS (4B)
------------	------------	-------------------------	-------------------------	--------------------------	------------------------	-------------

Untagged and Unencapsulated Layer 2 Frame from an Access Port

DA (6B)	SA (6B)	Len/Etype (2B)	Data (0-1500B)	FCS (4B)
------------	------------	-------------------	-------------------	-------------

0103_018



Configuring Trunk link

```
Switch(config)#interface fastethernet 2/1
```

- Enters interface configuration mode

```
Switch(config-if)#switchport trunk encapsulation isl/dot1q
```

- Selects the encapsulation

```
Switch(config-if)#switchport mode trunk
```

- Configures the interface as a Layer 2 trunk

```
Switch#show running-config interface {fastethernet | gigabitethernet}
slot/port
```

```
Switch#show interfaces [fastethernet | gigabitethernet] slot/port [ switchport
| trunk ]
```

```
Switch#show interfaces fastethernet 2/1 trunk
```

Port	Mode	Encapsulation	Status	Native VLAN
Fa2/1	desirable	isl	trunking	1

Port	VLANs allowed on trunk
Fa2/1	1-1005

Port	VLANs allowed and active in management domain
Fa2/1	1-2,1002-1005

Port	VLANs in spanning tree forwarding state and not pruned
Fa2/1	1-2,1002-1005

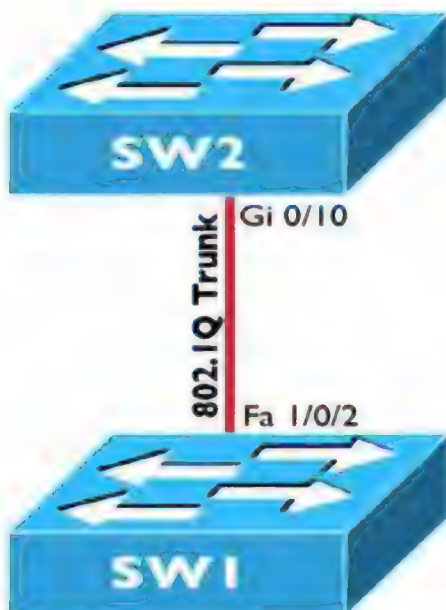


- Dynamic Trunking protocol is a dynamic way of establishing a trunk between two switches.
- DTP works in two modes
 - 1) Dynamic Desirable
 - 2) Dynamic Auto



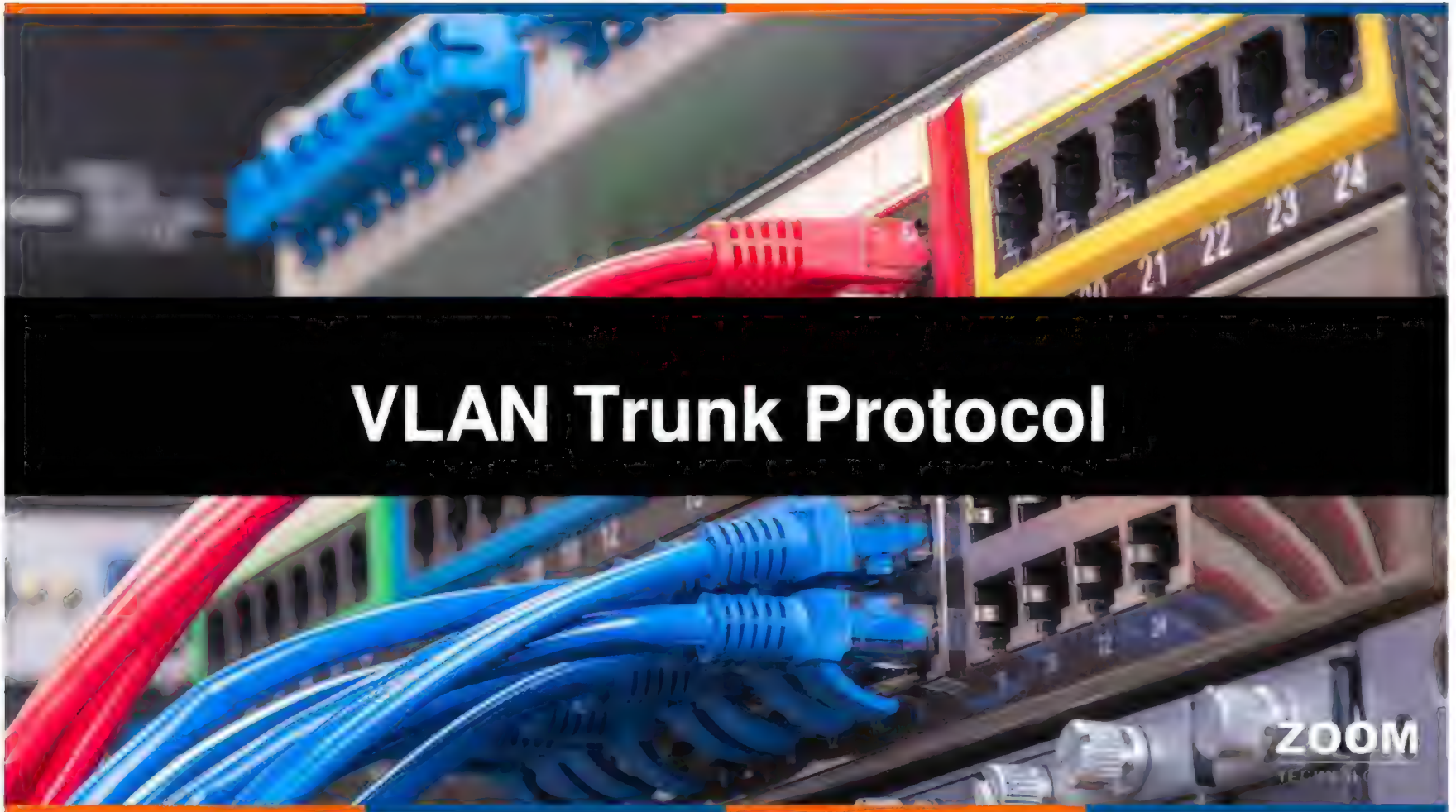
```
Switch(conf)#interface fastethernet 0/1
Switch(conf-if)#switchport nonegotiate
```

Zoom Technologies



Mode	Description
access	Forces a port to operate as an access port.
trunk	Forces a port to operate as a trunk port.
dynamic desirable	Initiates the negotiation of a trunk.
dynamic auto	Passively waits for the remote switch to initiate the negotiation of a trunk.

SW1 Mode	SW2 Mode	Trunk Formed
access	ANY	✗
trunk	dynamic desirable	✓
trunk	dynamic auto	✓
trunk	trunk	✓
dynamic desirable	dynamic desirable	✓
dynamic desirable	dynamic auto	✓
dynamic auto	dynamic auto	

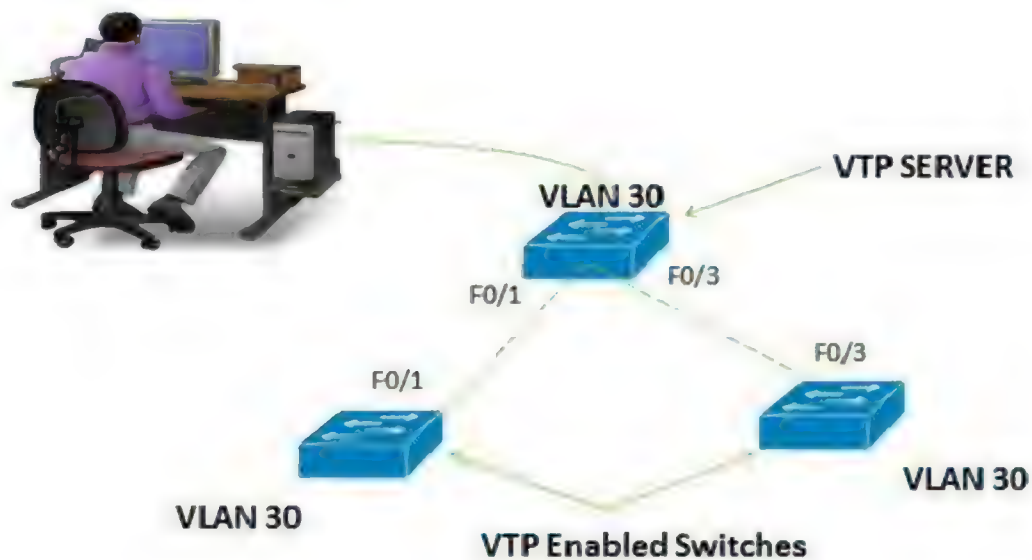


Purpose of VTP

ZOOM
TECHNOLOGIES

- You can create VLANs on a switch.
- What if you have the same VLANs on 10 linked switches? Or 100 linked switches?
- Do you have to create the VLANs on every switch and allow them on each trunk?
- VTP helps.
- But you still have to assign access ports to VLANs on each switch.





VTP Protocol Features

- VTP is a Cisco proprietary protocol.
- VTP is used to exchange vlan information between switches.
- Sends VTP advertisements on trunk ports only
- VTP reduces administration in a switched network.
- Maintains VLAN configuration consistency throughout a common administrative domain

Note: VTP will not assign vlan's to the ports.

VTP Server

- Create Vlans
- Delete Vlans
- Modify Vlans
- Sends and Forwards Advertisements
- Synchronizes

VTP Client

- Cannot create, delete and modify Vlans
- Forward Advertisements
- Synchronizes



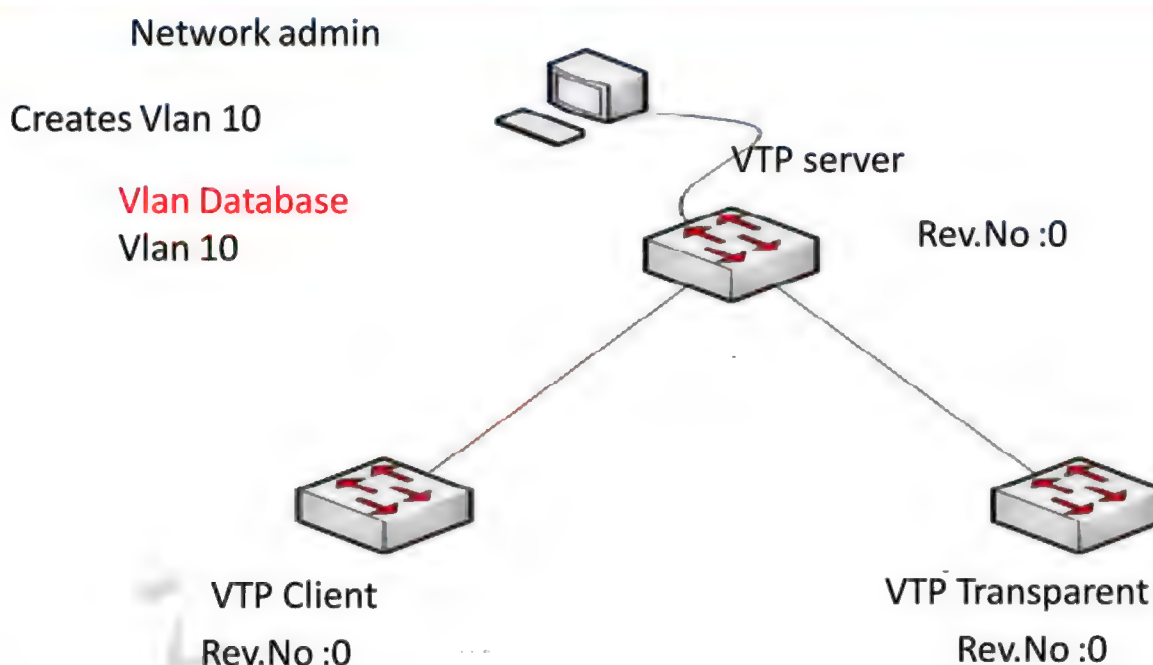
VTP Transparent

- Create, delete and modify Vlans local to the switch
- Forward Advertisements
- Does not synchronize



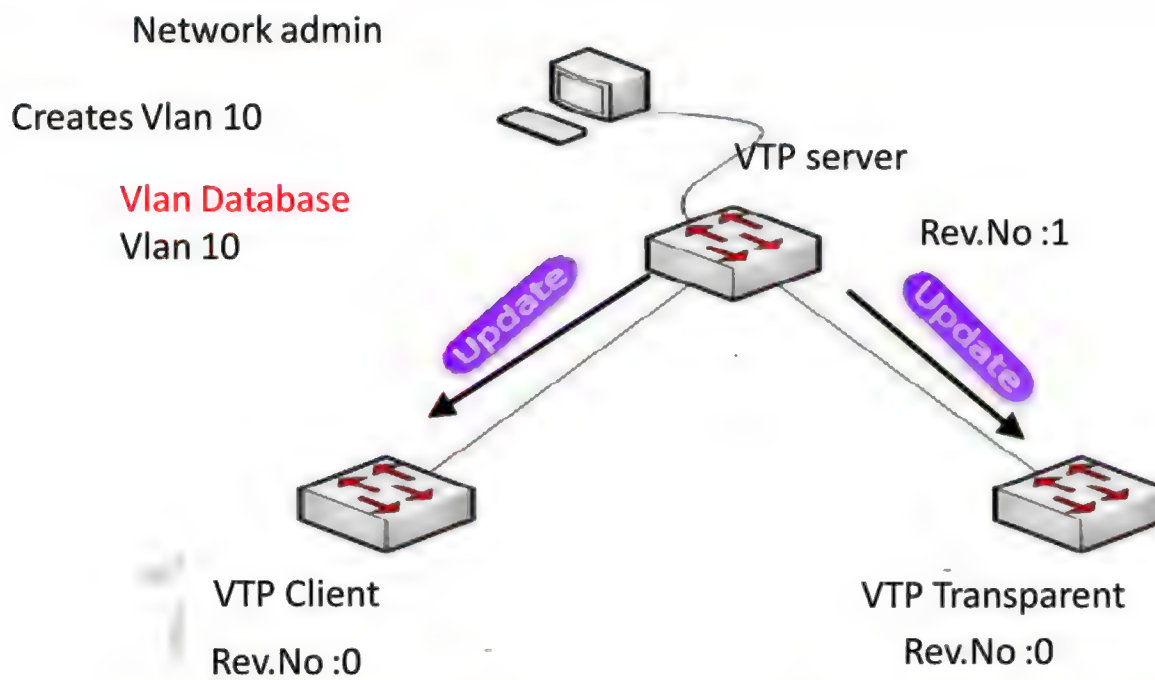
- VTP works based upon configuration revision number.
- Configuration revision number increases by one every time we create, delete and modify vlans on the sever.
- Configuration revision number ranges from 0-65,535
- This ensures that each switch participating in VTP always has the latest information – comparing the current configuration revision number with the received update , the update will be accepted only if it has a greater configuration revision number
- Configuration revision number of transparent switch always zero.

Working of VTP



Working of VTP

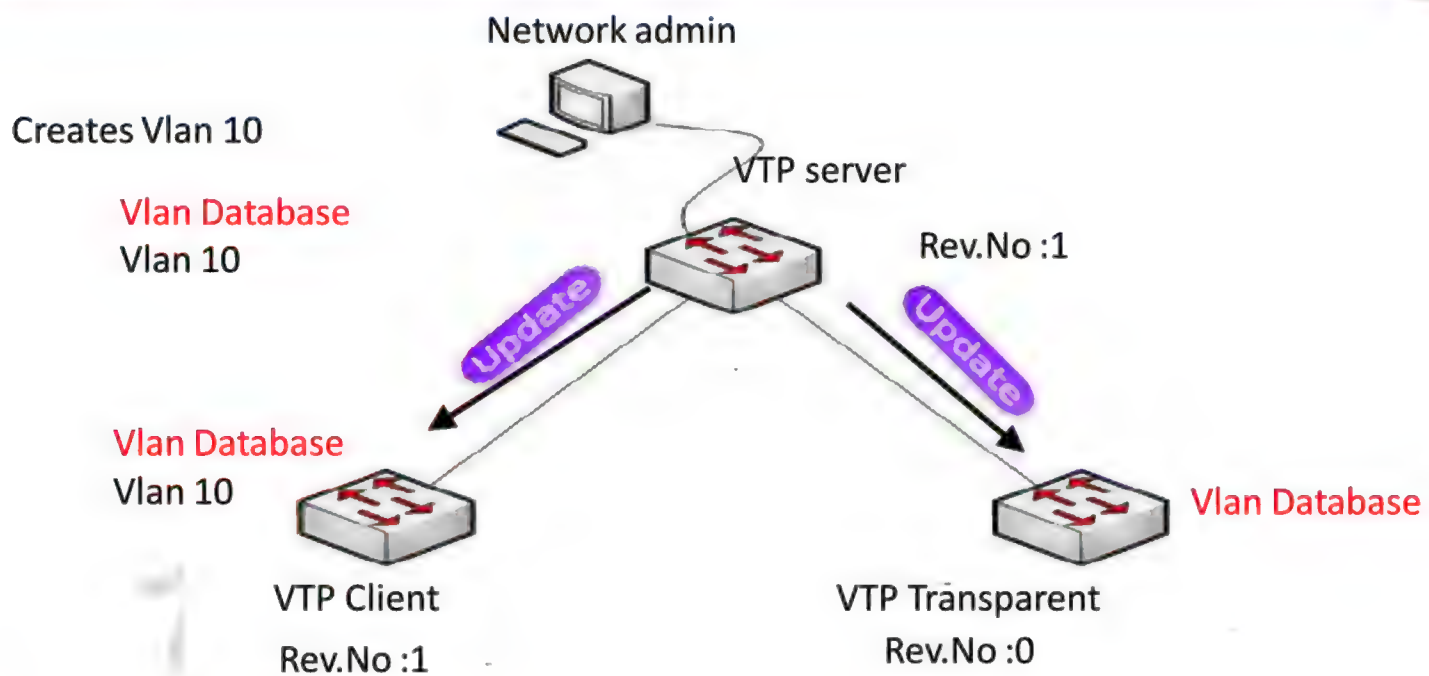
ZOOM
TECHNOLOGIES



CCIE
CCNP
CCNA

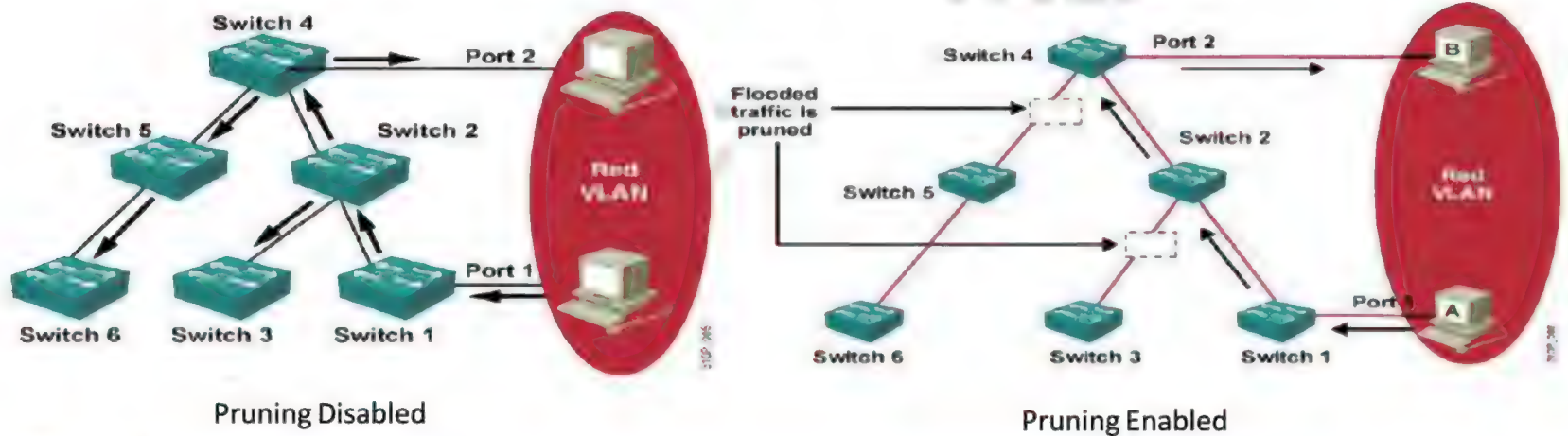
Working of VTP

ZOOM
TECHNOLOGIES



CCIE
CCNP
CCNA

- Uses bandwidth more efficiently by reducing unnecessary flooded traffic
- Example: Station A sends broadcast; broadcast flooded only toward any switch with ports assigned to the red VLAN



Configuring a VTP Server

```
Switch(config)#vtp mode server
```

- Configures VTP server mode

```
Switch(config)#vtp domain domain-name
```

- Specifies a domain name

```
Switch(config)#vtp password password
```

- Sets a VTP password

```
Switch(config)#vtp pruning
```

- Enables VTP pruning in the domain

```
Switch#show vtp status
```

```
Switch#show vtp status
```

```
VTP Version                : 2
Configuration Revision      : 247
Maximum VLANs supported locally : 1005
Number of existing VLANs    : 33
VTP Operating Mode          : Client
VTP Domain Name             : Lab_Network
VTP Pruning Mode            : Enabled
VTP V2 Mode                  : Disabled
VTP Traps Generation        : Disabled
MD5 digest                  : 0x45 0x52 0xB6 0xFD 0x63 0xC8 0x49 0x80
Configuration last modified by 0.0.0.0 at 8-12-99 15:04:49
```

```
Switch#
```

CCNP
CCNA

VTP Advertisements

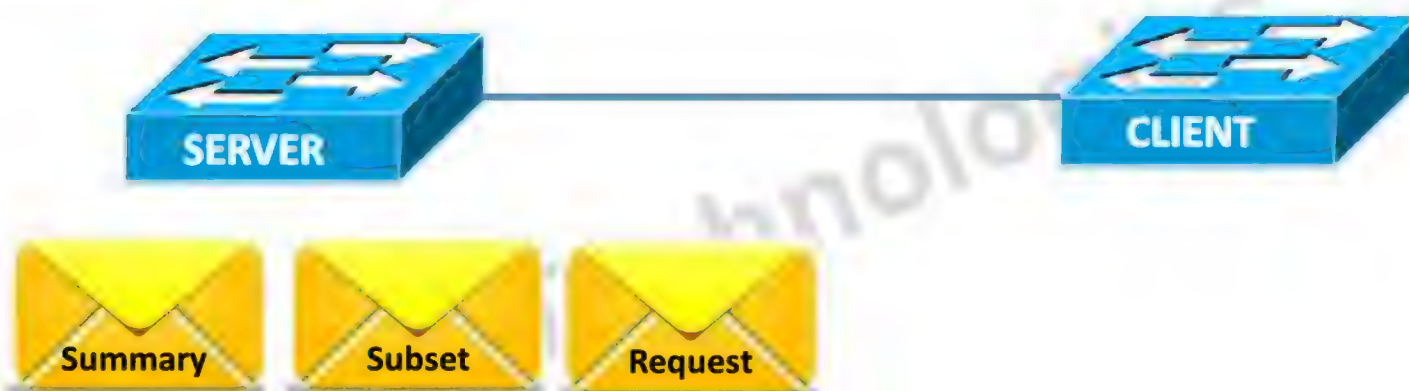
1) Summary Advertisements

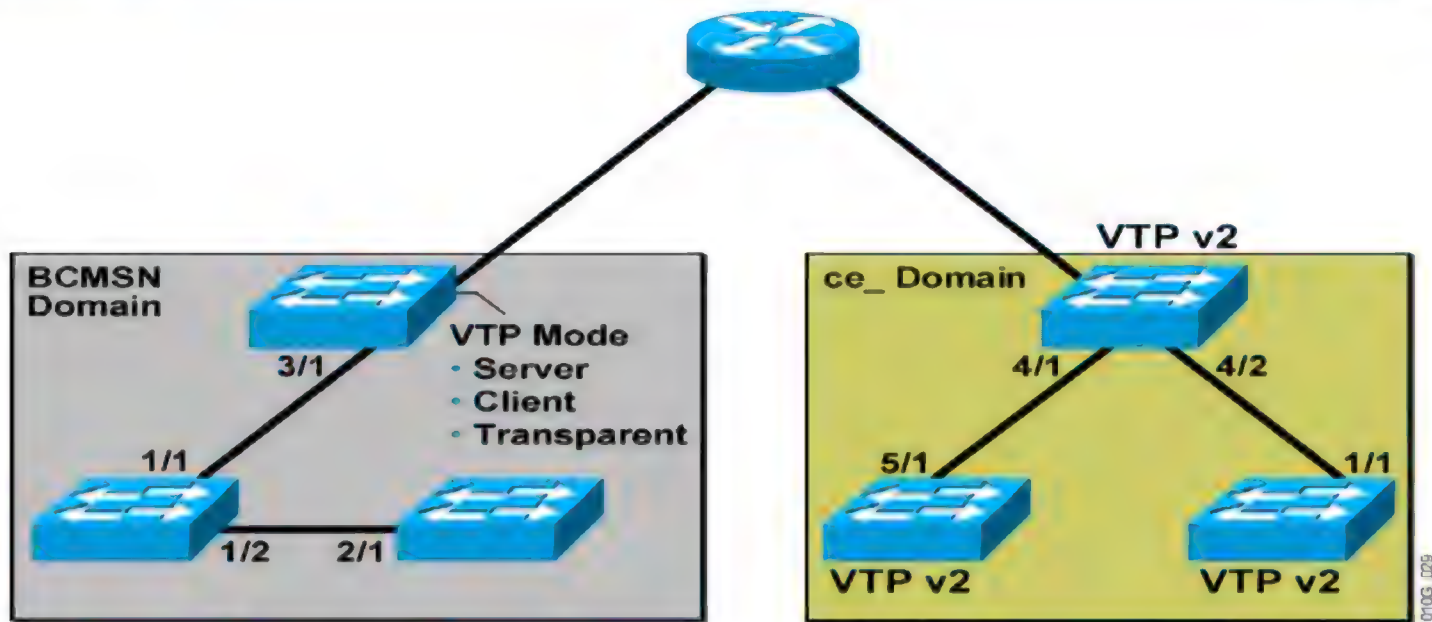
CCIE
CCNP
CCNA

2) Subset Advertisements



3) Request Advertisement





- All switches in a management domain must run the same version.

- In VTP version 1 and 2, VTP client can override vlan information in VTP server if it has higher configuration revision number compared to server.
- It is recommended to add new switch to the switched network in VTP client with revision number zero.
- VTP version 3 overcomes this problem
- VTP version 3 supports password encryption.

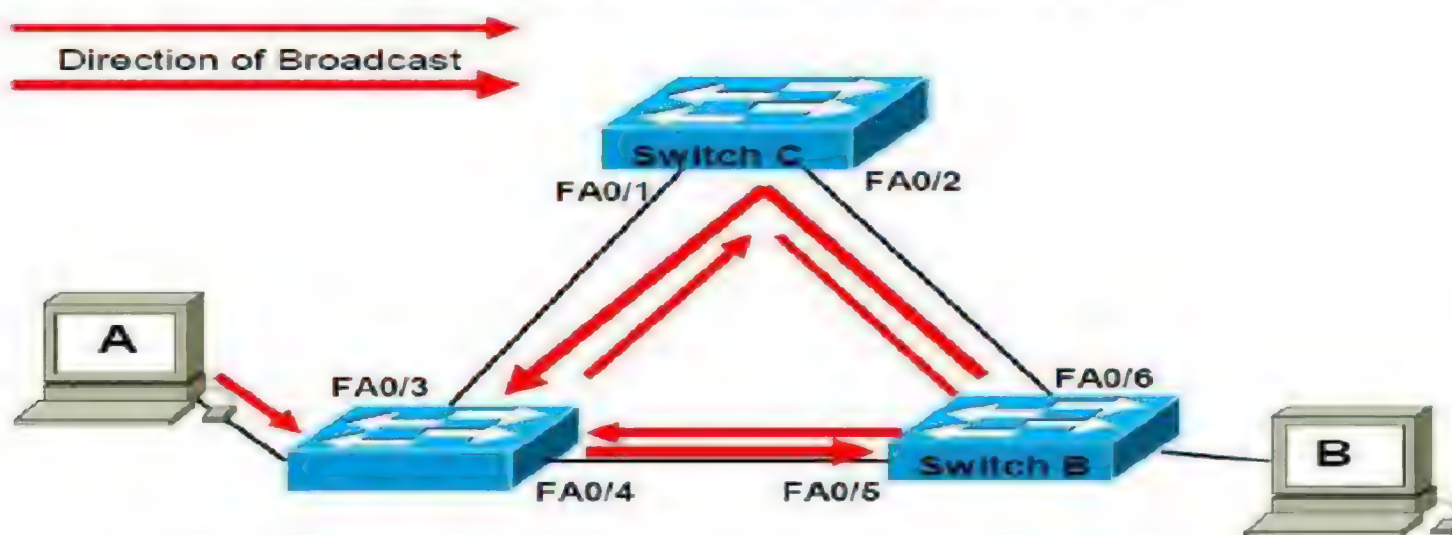
Spanning Tree Protocol

ZOOM

Bridging Loops

ZOOM
TECHNOLOGIES

Broadcast Storm



- Host A sends a broadcast.
- Switches continue to propagate broadcast traffic over and over

Spanning Tree Protocol



- STP is open standard protocol(IEEE 802.1D)
- It blocks all the redundant paths and provides a loop free L2 path
- STP uses Spanning Tree Algorithm(STA) to provide loop free topology
- “Radia Perlmán” is the inventor of the spanning tree algorithm
- Enabled by default on all Cisco switches



STP Election



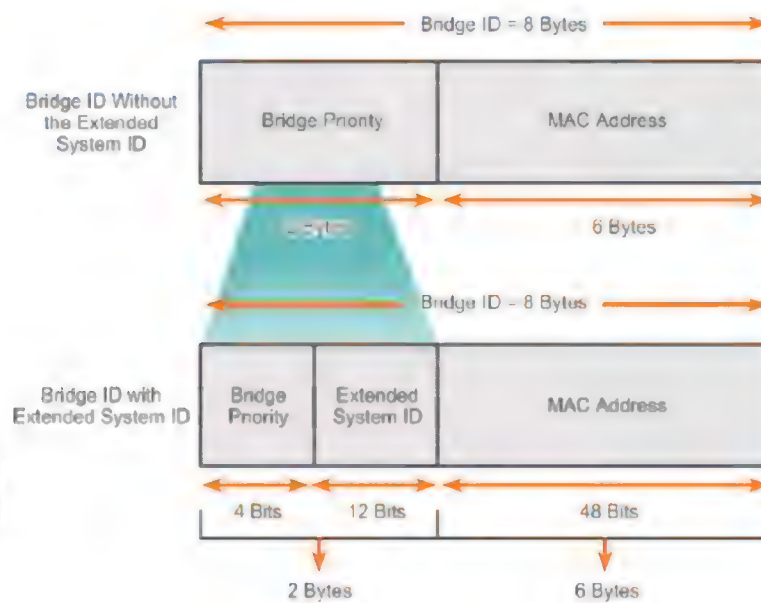
- Election of Root Bridge
 - Lowest Bridge ID (MAC address + Priority)
- Election of Root Port on Non Root Switch
 - Lowest Path cost (total cost to reach root switch)
 - Lowest sender bridge id
 - Lowest Port ID (Port Number)
- Election of Designated Port on Non Root Switch
 - Lowest Path cost
 - Lowest sender bridge id
 - Lowest Port ID

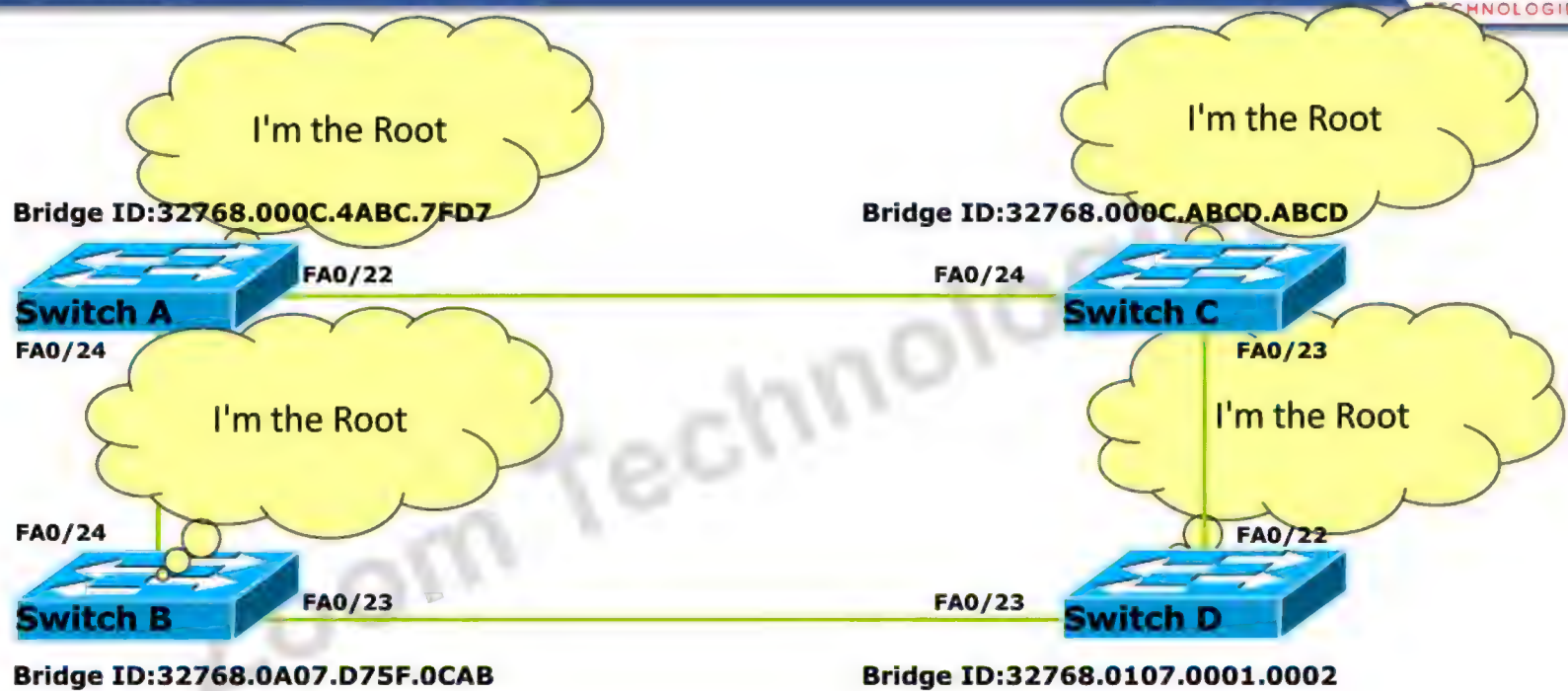
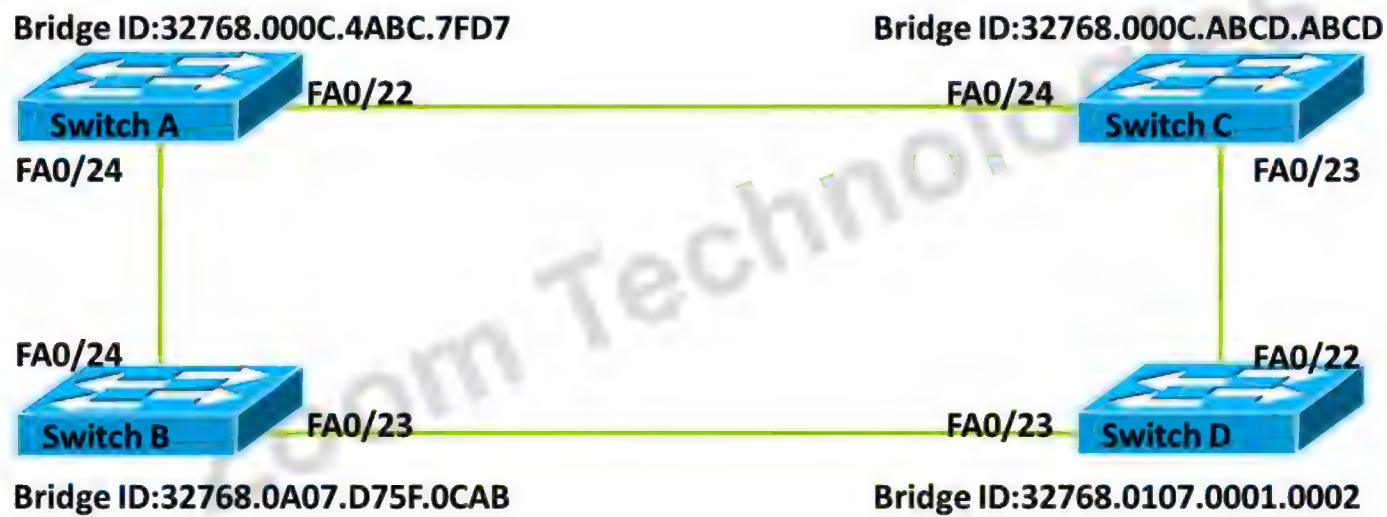


STP Cost

Speed	Cost
10 Mbps	100
100 Mbps	19
1000 Mbps	4
10000 Mbps	2

Bridge ID

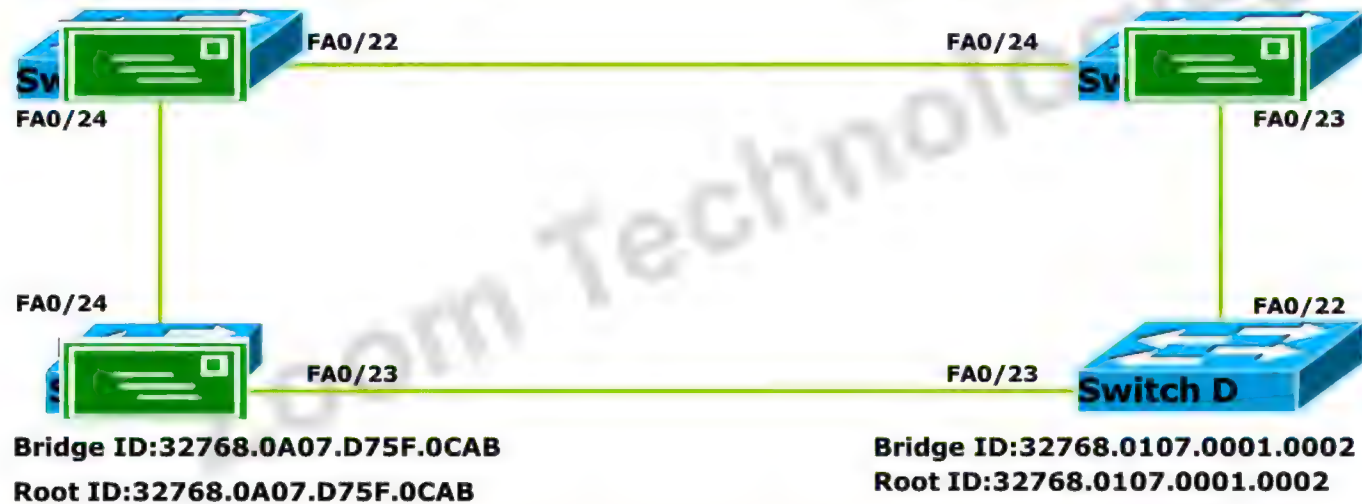




STP Election

Root ID:32768.000C.4ABC.7FD7
Bridge ID:32768.000C.4ABC.7FD7

Root ID:32768.000C.ABCD.ABCD
Bridge ID:32768.000C.ABCD.ABCD



STP Election

Root ID:32768.000C.4ABC.7FD7
Bridge ID:32768.000C.4ABC.7FD7

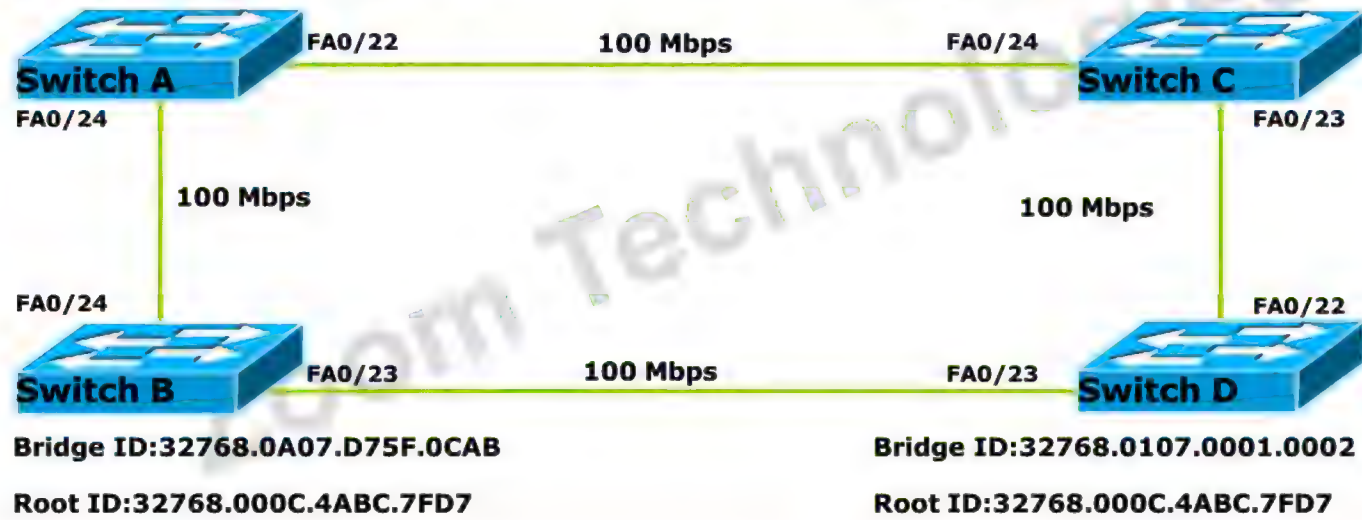
Root ID:32768.000C.4ABC.7FD7
Bridge ID:32768.000C.ABCD.ABCD



STP Election

Root ID:32768.000C.4ABC.7FD7
Bridge ID:32768.000C.4ABC.7FD7

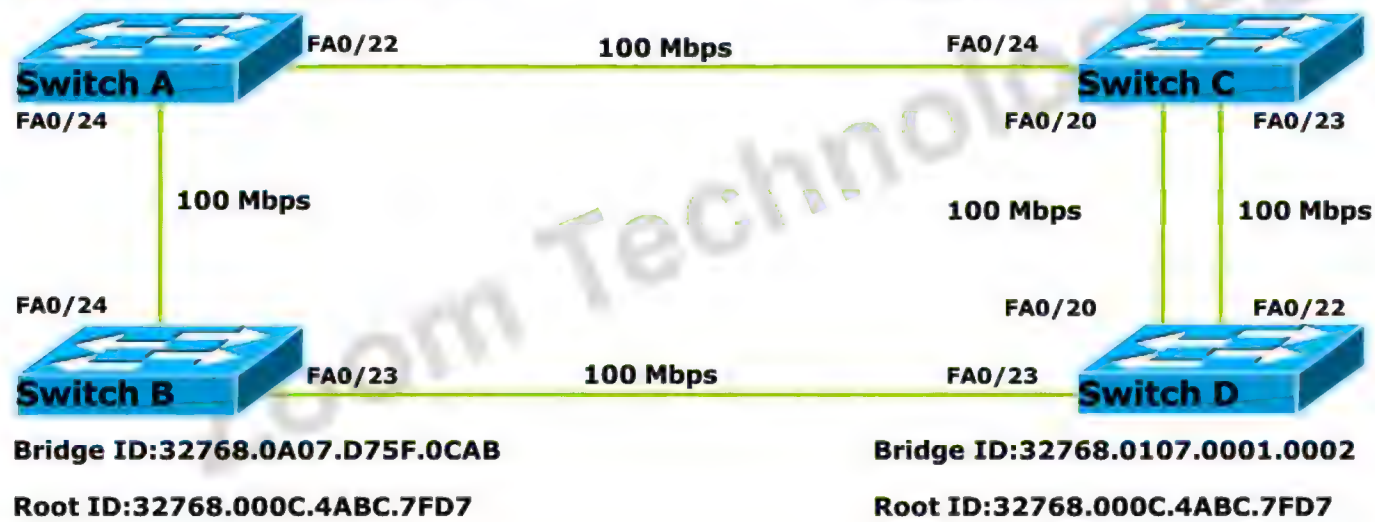
Root ID:32768.000C.4ABC.7FD7
Bridge ID:32768.000C.ABCD.ABCD

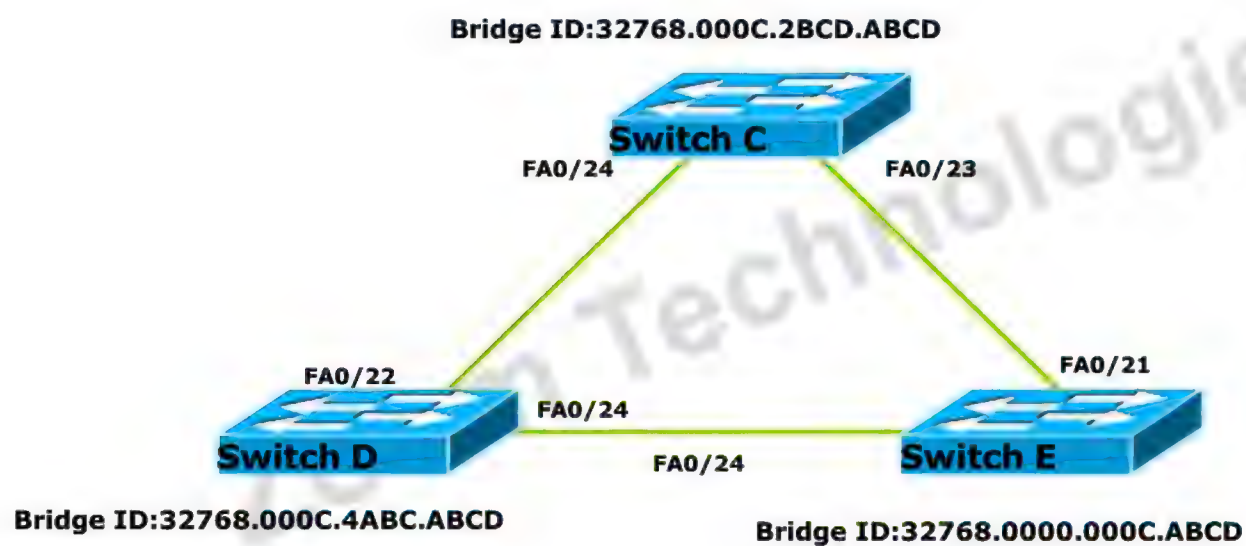


STP Election

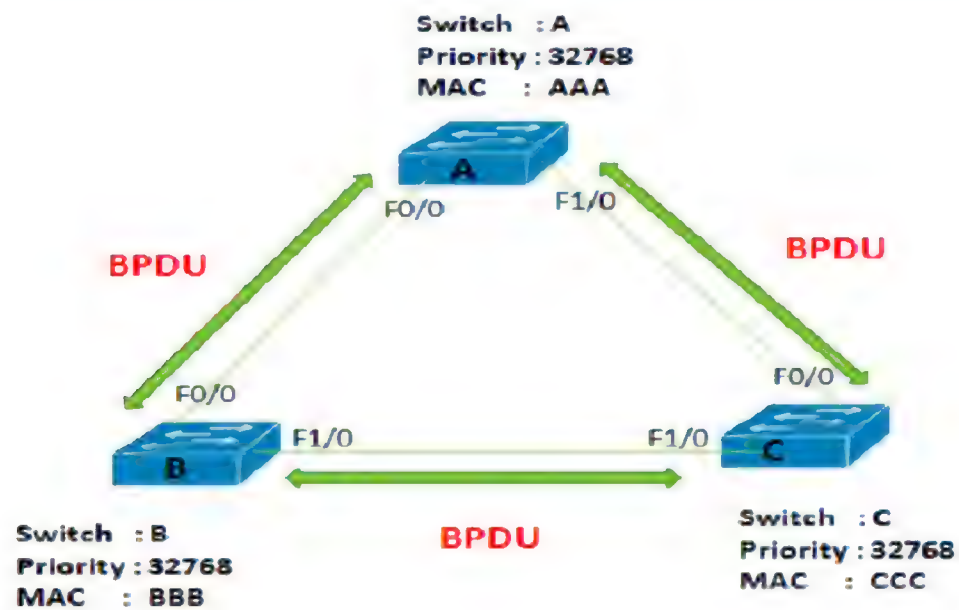
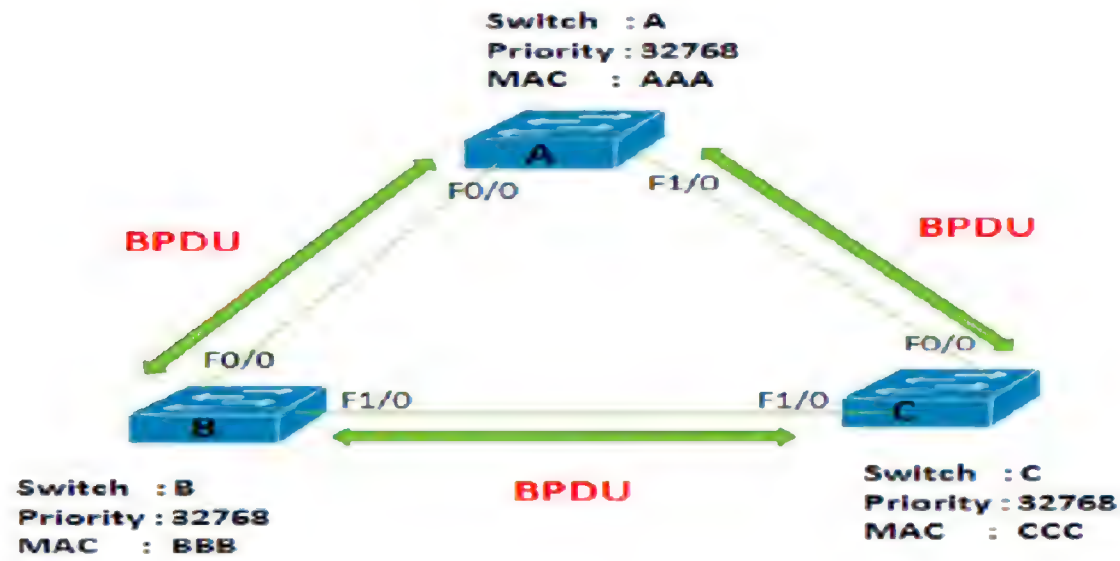
Root ID:32768.000C.4ABC.7FD7
Bridge ID:32768.000C.4ABC.7FD7

Root ID:32768.000C.4ABC.7FD7
Bridge ID:32768.000C.ABCD.ABCD





- STP uses BPDU's (Bridge Protocol Data Unit) to find redundant links that will cause loop in switched networks.
- Switches send BPDU frame on multicast address 01:80:C2:00:00:00



- Configuration BPDU
- Topology Change Notification BPDU
- Topology Change Acknowledgement BPDU

Protocol	Version	Message type	Root ID	Cost	Bridge ID	Port ID	Message Age	Max Time	Hello	Forward Delay
1 B	1 B	1 B	8 B	4 B	8 B	2 B	2 B	2 B	2 B	2 B

- **Disabled State:**
 - Layer 2 port does not participate in spanning tree and does not forward frames.
- **Blocked State:**
 - Only receives BPDU's
 - Stays for 20 sec
- **Listening State:**
 - Receives and Sends BPDU's
 - Stays for 15 sec

- **Learning State:**
 - Receives and Sends BPDU
 - Learns Mac address
 - Stays for 15 sec
- **Forwarding State:**
 - Receives and Sends BPDU
 - Learns Mac address
 - Forwards data

•Hello Timer

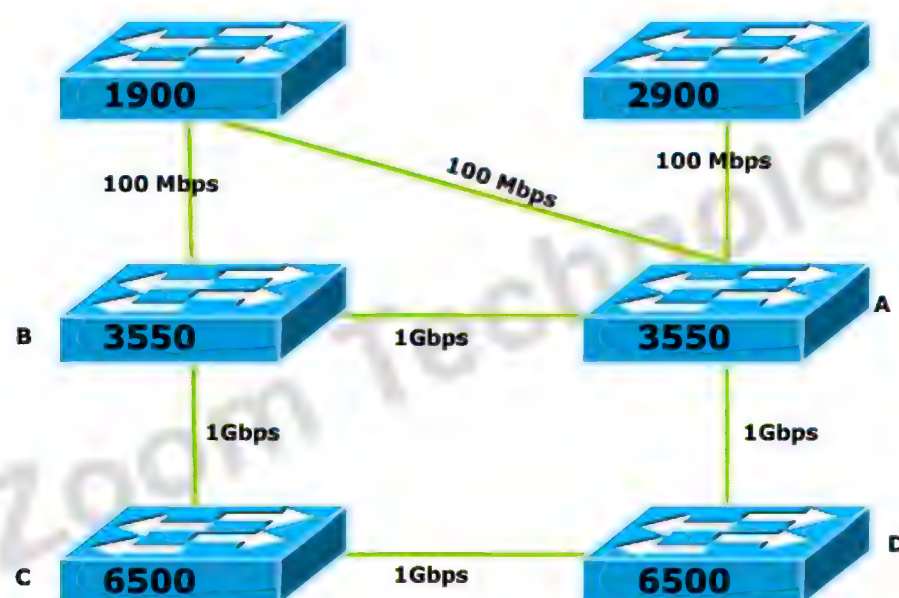
- Determines how often root bridge sends configuration BPDUs. The default is 2 seconds.

•Max Age

- how long to keep ports in the blocking state before listening. The default is 20 seconds.

•Forward Delay

- how long to stay in the listening state before going to the learning state, and how long to stay in the learning state before forwarding. The default is 15 seconds.



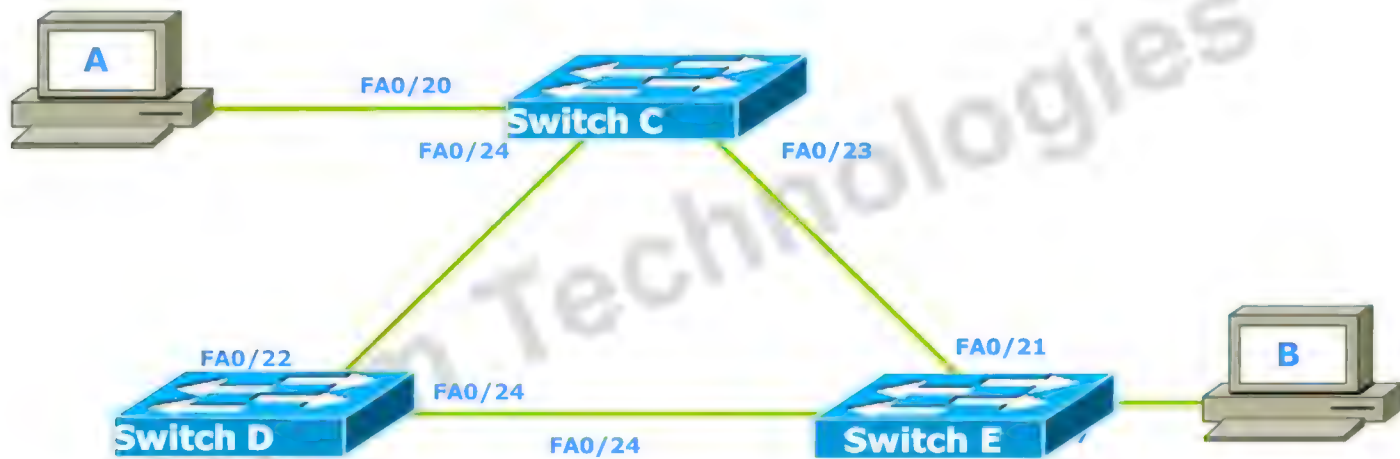


Enhancements to STP

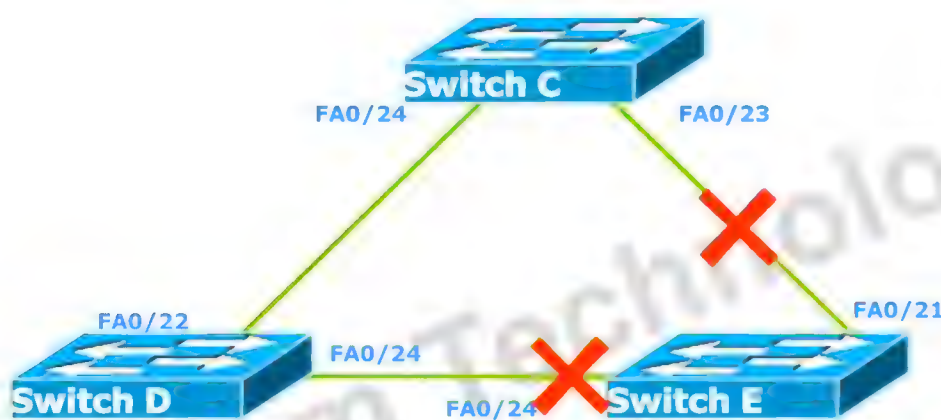
ZOOM
TECHNOLOGIES

- **Portfast**
 - used for Access ports
 - port state switched from Disable to Forwarding
 - No delay, saves 50 seconds
- **Uplinkfast**
 - configured on a switch with at least one Blocked port
 - the Blocked port switches to Forwarding state without any delay, saves 30 seconds
- **Backbonefast**
 - configured on all switches
 - if indirectly connected link fails, the switch with Blocked port switches to Forwarding state in 30 seconds, saves 20 seconds



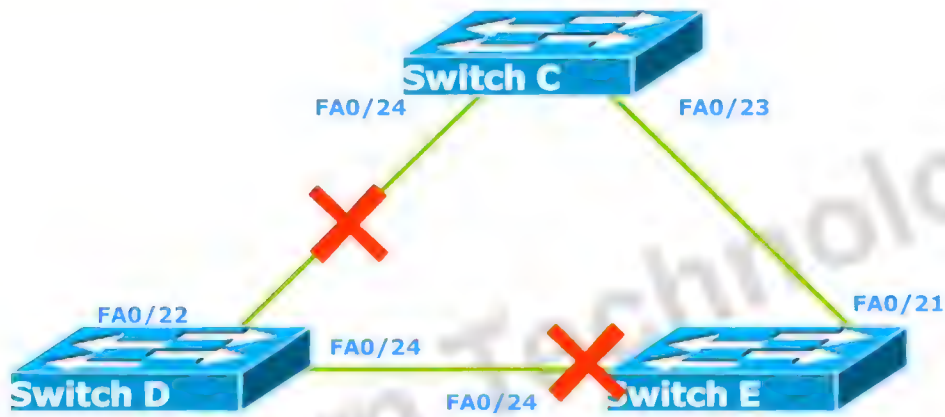


After Portfast is configured:
The port state switches from
Disable → Forwarding



After uplinkfast is
configured:
When root port is down

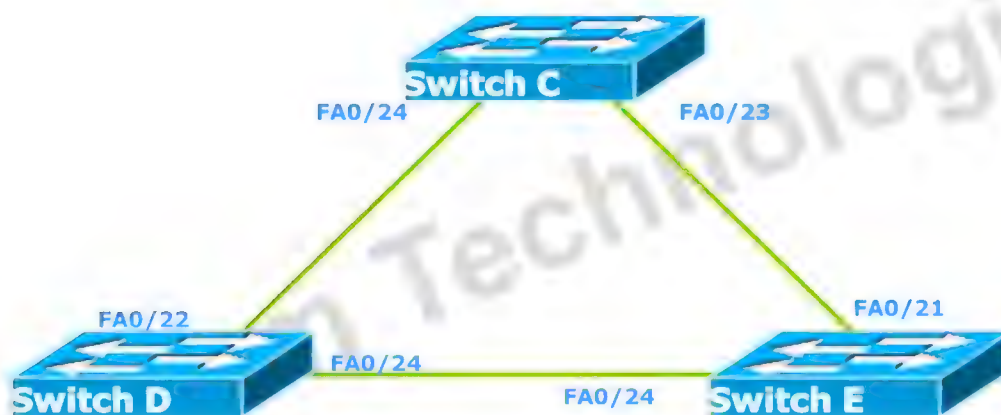
Block →
Forwarding

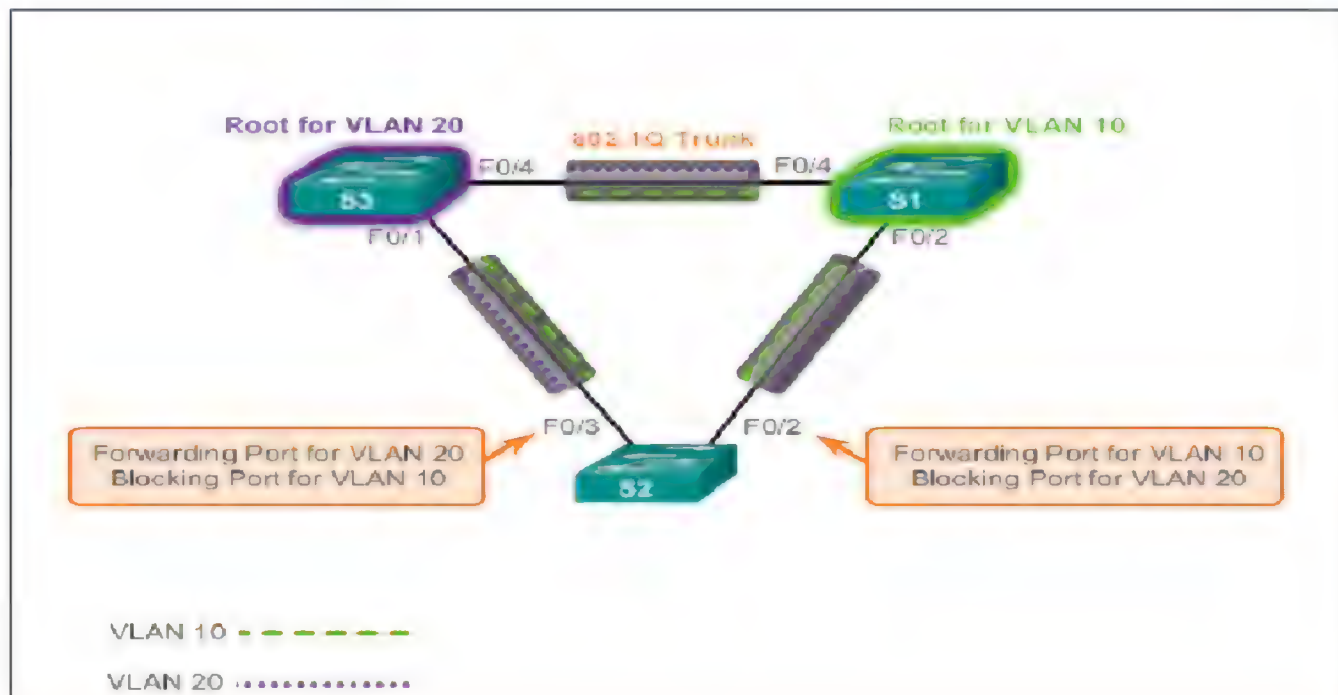


After backbone Fast
15 listening →
15 learning →
Forwarding state

Per-VLAN Spanning Tree - PVST

- Cisco proprietary
- Single STP instance for each VLAN
 - Separate BPDU, Roots and Blocked Port
- PVST work only on trunk link
- PVST works only ISL, PVST+ works on ISL/Dot1Q





Advanced Spanning Tree Rapid Spanning Tree Protocol

Rapid Spanning Protocol

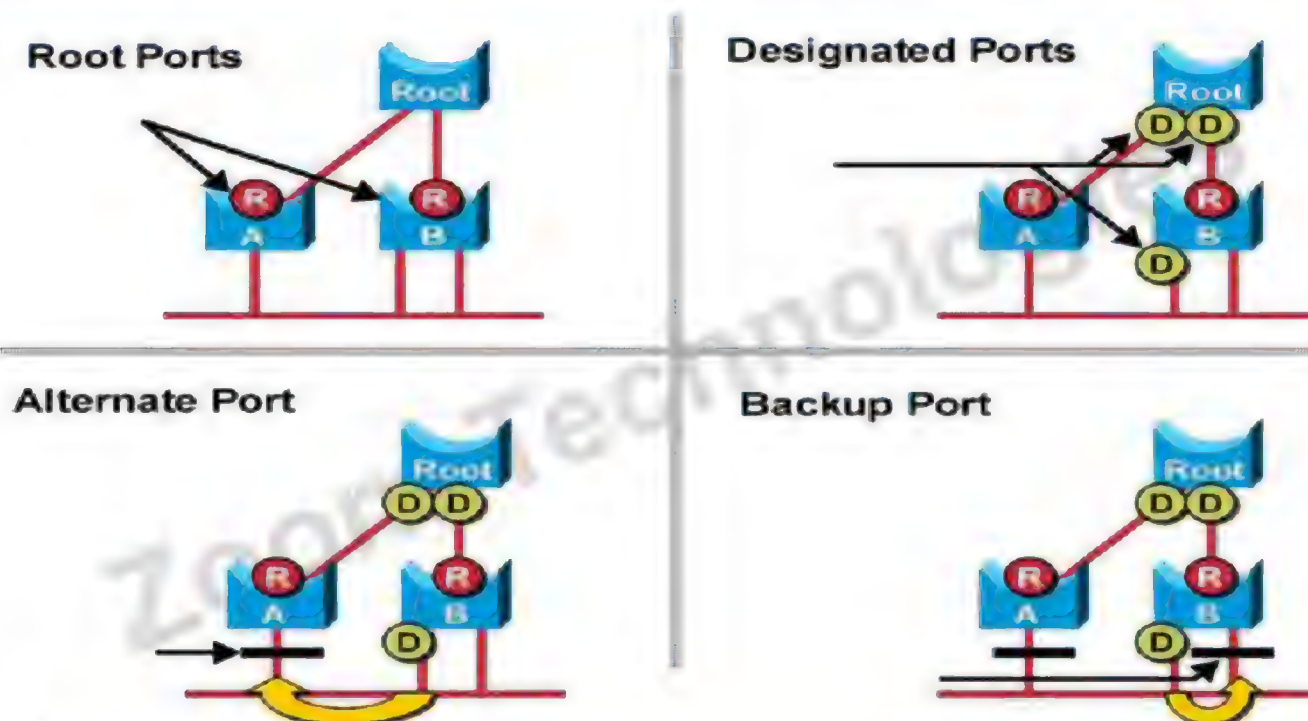
- Open Standard (IEEE 802.1w)
- RSTP is enhanced version of STP
- RSTP Election Process is similar to STP
- RSTP is backward compatible with STP 802.1D
- RSTP provides faster convergence
 - BPDU is send every 2 sec and hold 6 sec
 - Uplinkfast and Backbonefast are enabled by default

RSTP Port States

STP	RSTP
Disable	Discarding
Blocked	
Listening	
Learning	Learning
Forwarding	Forwarding

Port States

- **Discarding**
Prevents the forwarding of data frames.
- **Learning**
Accepts data frames to populate the MAC table.
- **Forwarding**
Forwards data frames and determines the topology.

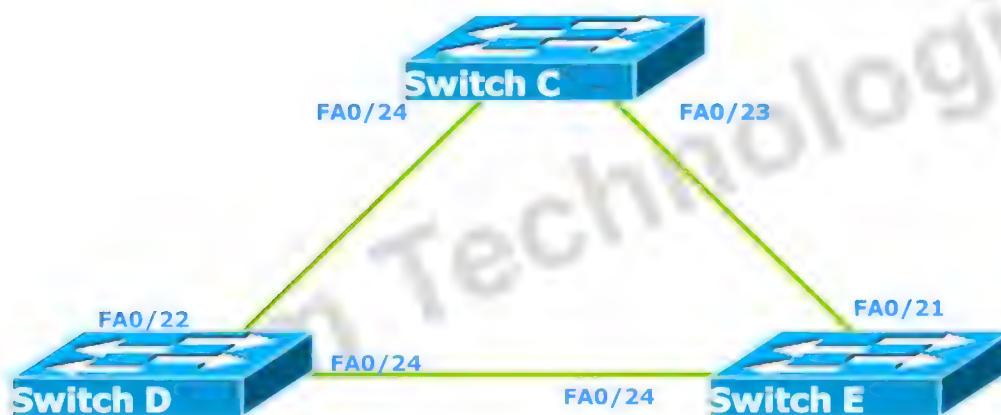


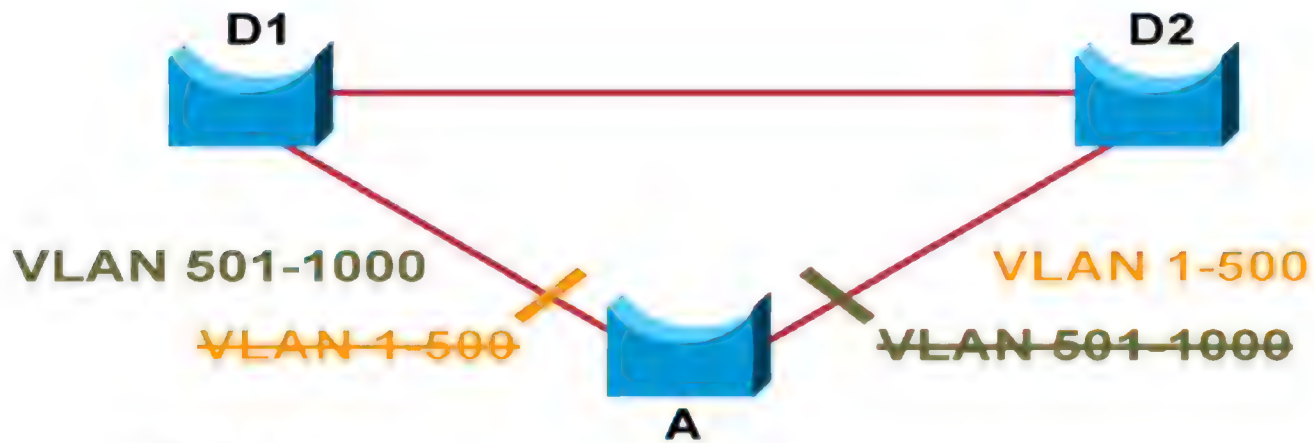
- Link Type in RSTP are
 - Edge port:
 - Port configured with Portfast command
 - Non Edge Port:
 - Port without a Portfast command
 - Non Edge port are of two type:
 - Point to Point : Full Duplex links
 - Shared : Half Duplex Link

Zoom Technologies

Multiple Spanning Tree (MST)

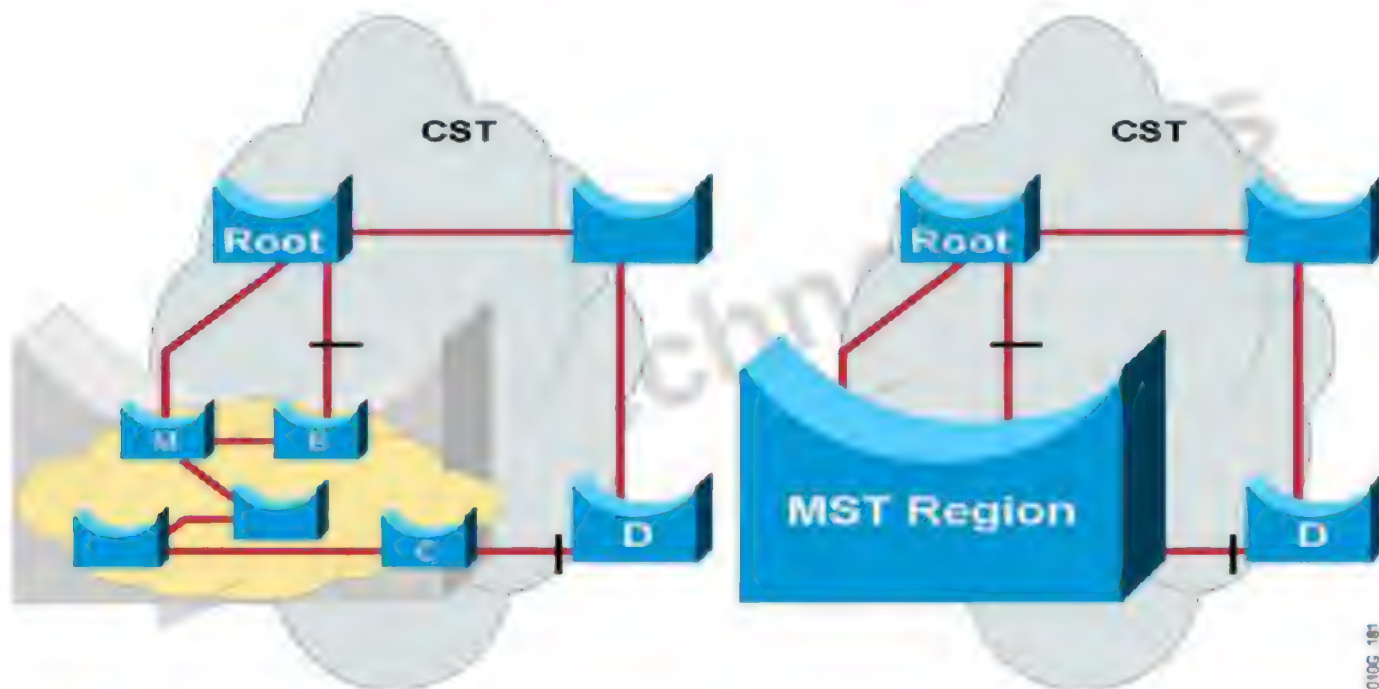
- Open Standard (IEEE 802.1s)
- One STP for a group of VLAN
- Also Know as Multiple instance of Spanning tree
- Backwards compatible with STP and RSTP





- MST configuration on each switch:
 - Name
 - Revision number
 - VLAN in Each Instance





0106_101

```
Switch(config)#spanning-tree mode mst
```

- Enables Multiple Spanning Tree

Switch(config)#spanning-tree mst configuration

- Enters MST configuration submode

Switch(config-mst)#name *name*

- Sets the MST region name

Switch(config-mst)#revision *rev_num*

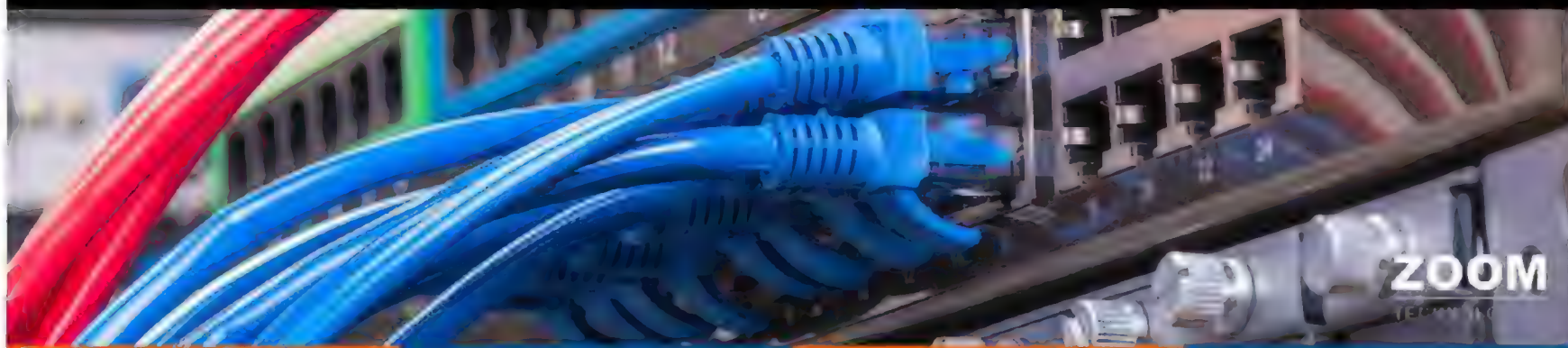
- Sets the MST configuration revision number

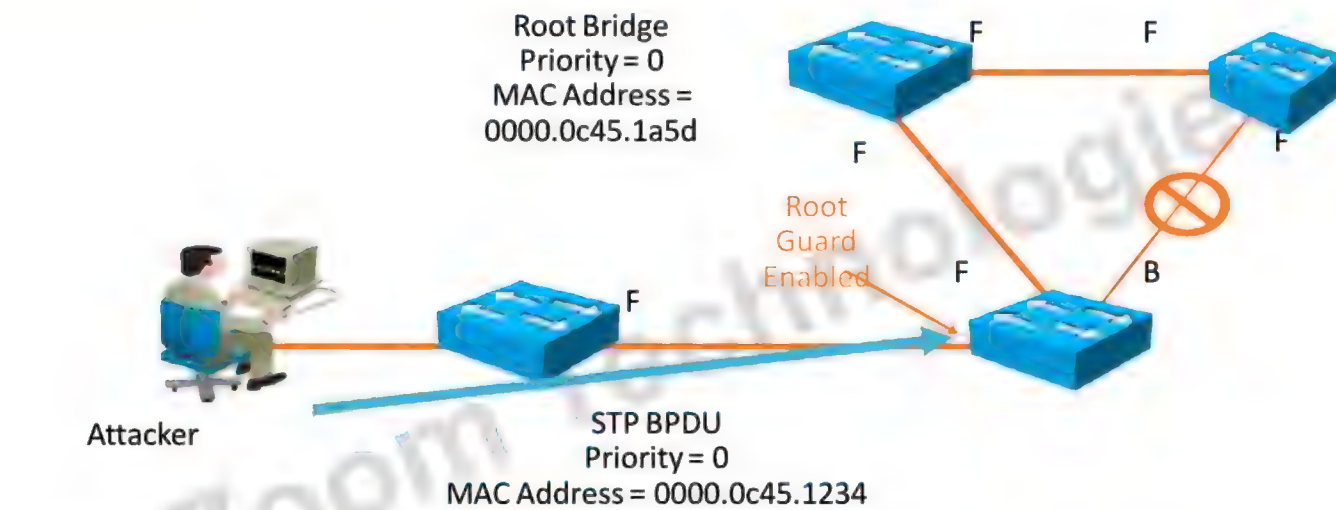
Switch(config-mst)#instance *inst* vlan *range*

- Maps the VLANs to an MST instance



Protecting Against Unexpected BPDU



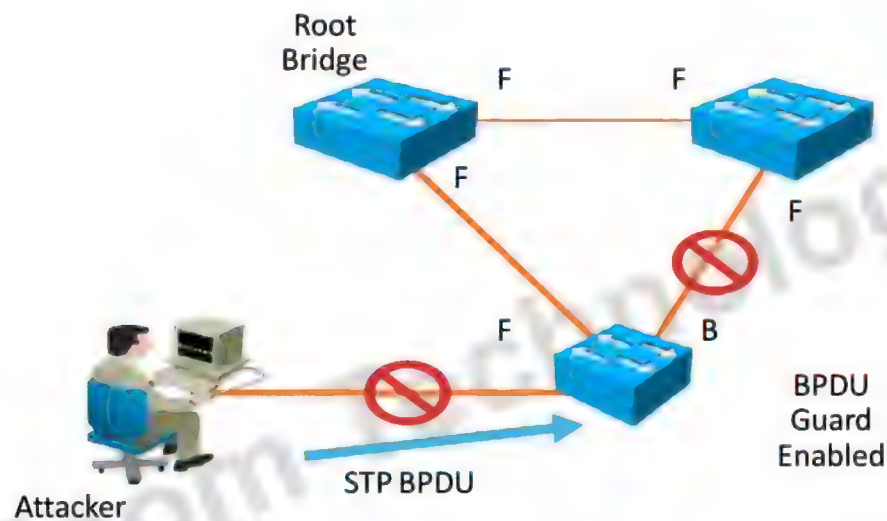


Switch(config-if)#

spanning-tree guard root

- Enables root guard on a per-interface basis

- BPDU guard places a PortFast port into blocking state if a BPDU is received on that port
- If a switch is attached to a port configured with Port Fast a layer 2 loop may occur, followed by a broadcast storm
- Protects a port configured with PortFast



Switch(config)#

spanning-tree portfast bpduguard default

- Globally enables BPDUGuard on all ports with PortFast enabled

- BPDUGuarding allows a switch to stop sending/receiving BPDUs on a port depending on how is configured.
- BPDUGuarding configured on the interface level will completely stop sending and receiving of BPDUs.
- BPDUGuarding configured on the Global configuration level will remove the port fast state and transition the port through normal STP states.
- SwitchB(config-if)#spanning-tree bpduguard enable



Protecting Against Sudden Loss Of BPDUs

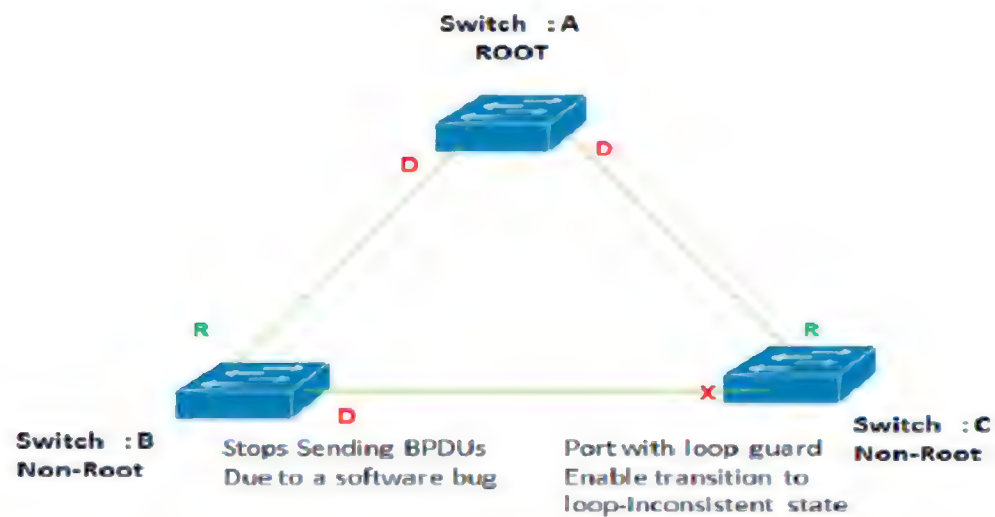
Loop Guard

ZOOM
TECHNOLOGIES

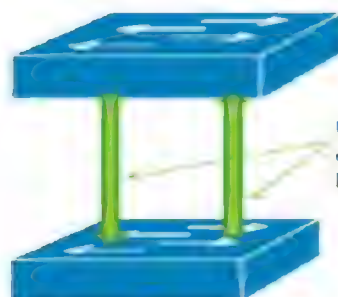
- Loop guard helps prevent bridging loops that could occur because of Software and Hardware failure
- High CPU utilization may prevent BPDUs from being received or processed.
- Loop Guard will place the interface in the loop-inconsistent state.
- Switch(config-if)# spanning-tree guard loop



Loop Guard



- UDLD is similar to loop guard used to prevent loops caused by unidirectional links.
- UDLD is typically used on fiber links.
- Switch(config)#udld enable



Unidirectional Fiber links the failure either of either causes a potential loop.



Routing Between VLANs

Inter Vlan Routing

ZOOM
TECHNOLOGIES

- By default Layer 2 switch cannot forward the traffic between two different vlans.
- A layer 3 device is required to forward the traffic between two different vlans.
- A layer 3 device can be
 - Router
 - Multi Layer Switch



- Legacy Inter Vlan Routing
- Router On a Stick
- Multilayer Switch

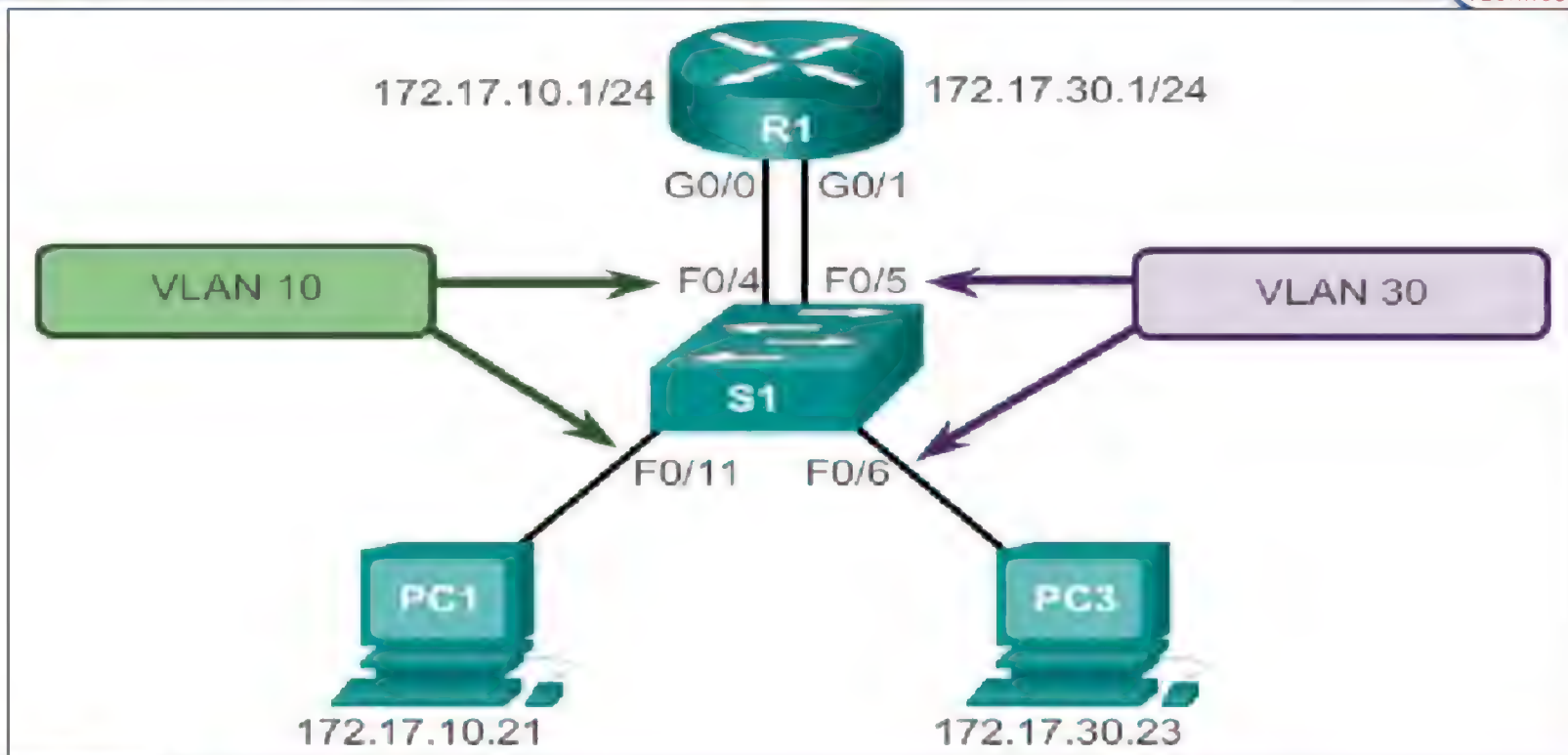
Zoom Technologies



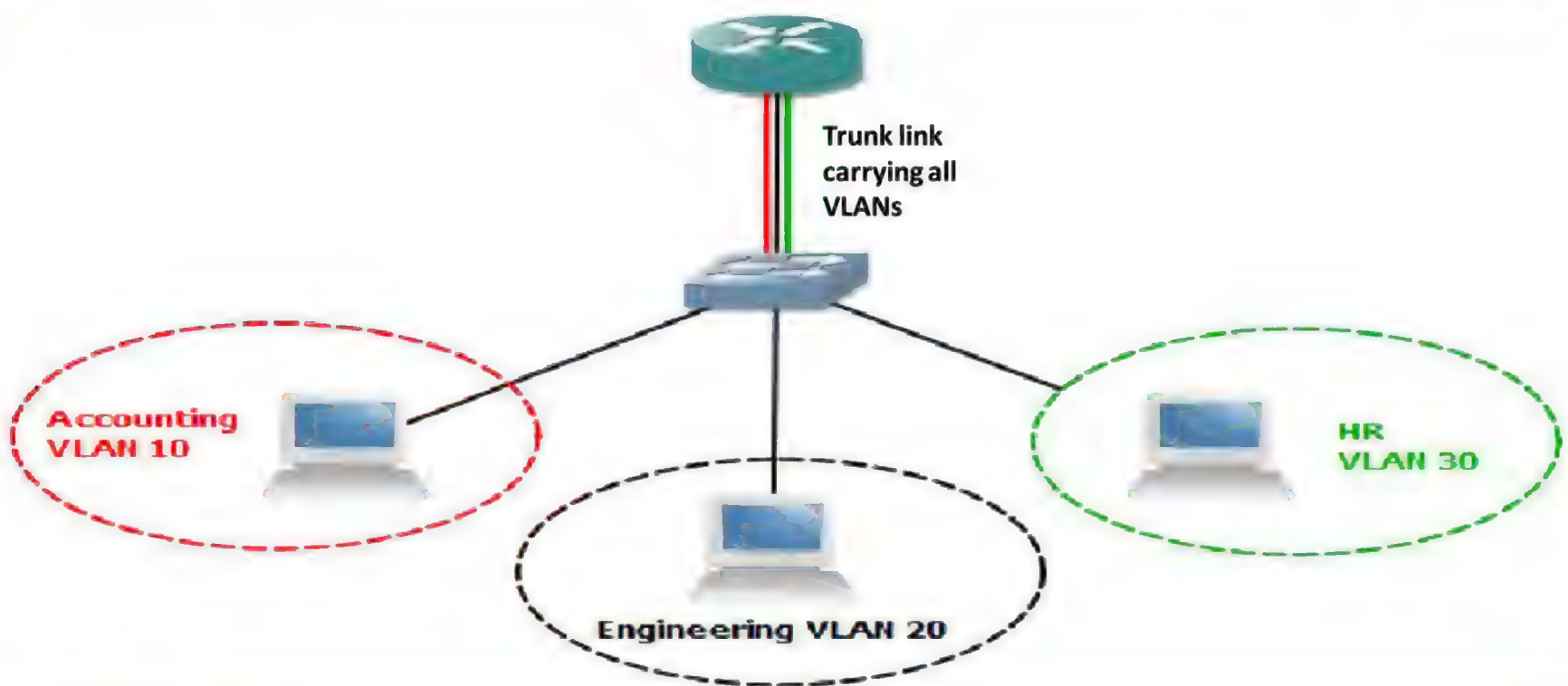
- It is also called as traditional inter vlan routing.
- Uses Router to perform Inter Vlan Routing.
- Each vlan is connected to different physical interface of the router.
- Packets would arrive on the router through one interface, leave through another interface.
- Large networks with large number of VLANs require many router interfaces.

Zoom Technologies





- The router-on-a-stick approach uses a different path to route between VLANs.
- The Physical interface of the router is divided into one or more sub interfaces.
- Vlan's are assigned to sub interfaces instead of physical interfaces.
- Each sub interface is configured with an IP address for the VLAN it represents.
- Only one of the router's physical interface is used.

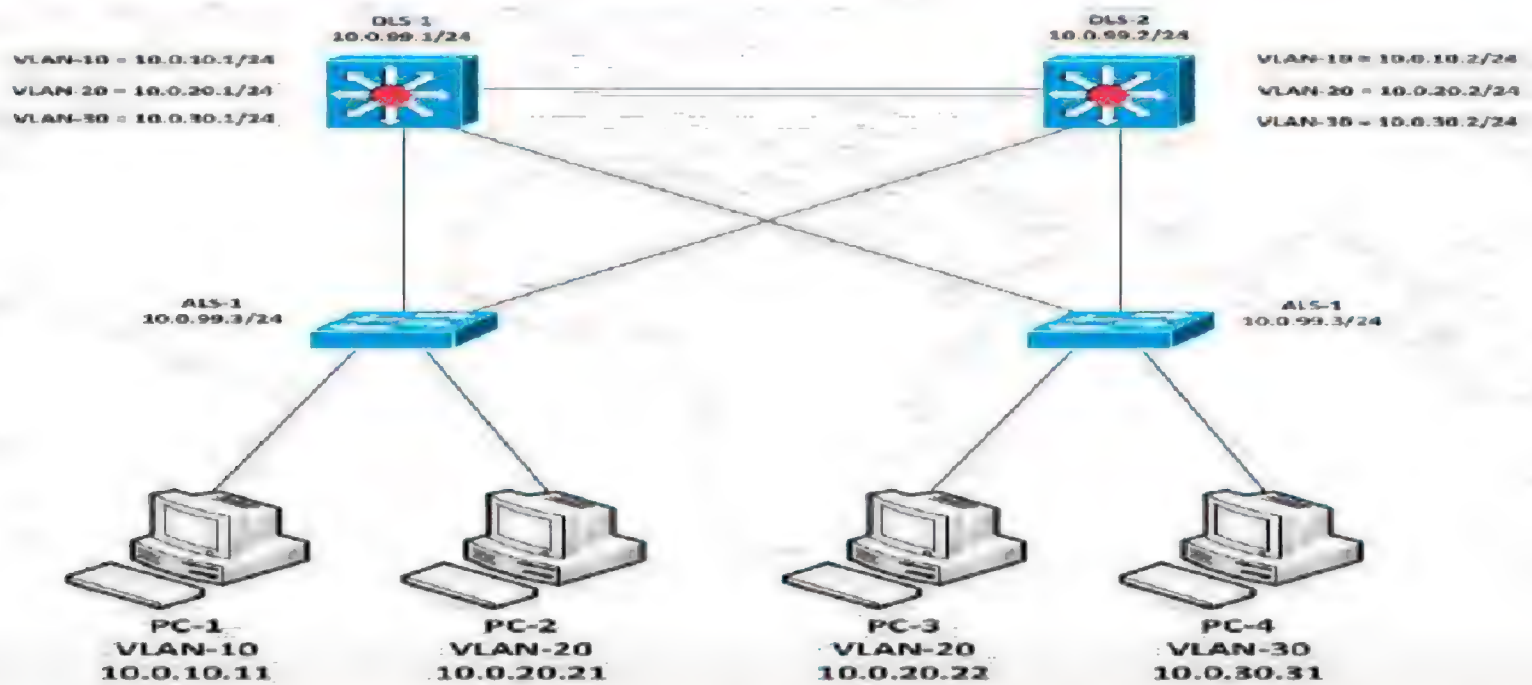


- Multi Layer Switch can perform layer 2 as well as layer 3 functions.
- Vlan's are assigned to Switch Virtual Interface(SVI).
- Each SVI is configured with an IP address for the VLAN it represents.
- This method uses ASIC to forward the traffic between vlans.

Zoom Technologies

Multi Layer Switching

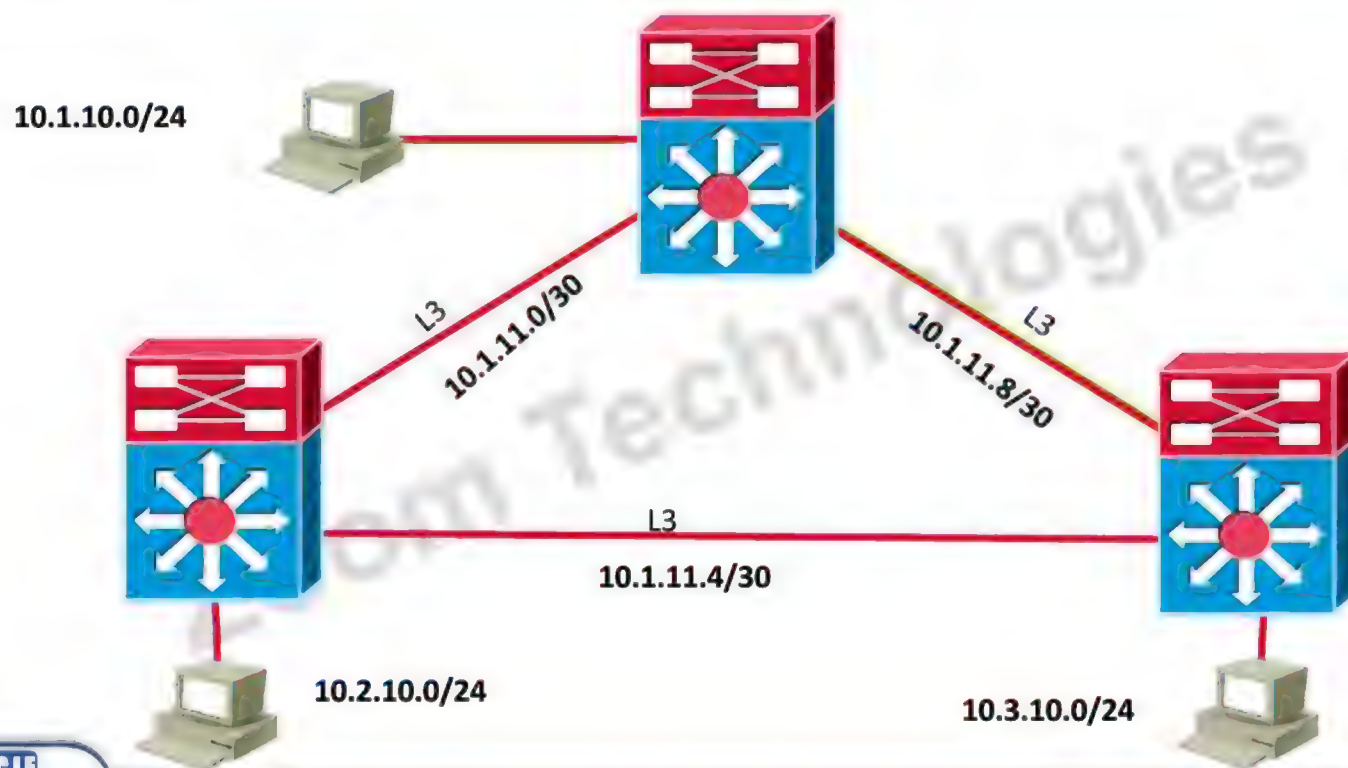
ZOOM
TECHNOLOGIES



CCIE
CCNP
CCNA

Multilayer Switch

ZOOM
TECHNOLOGIES



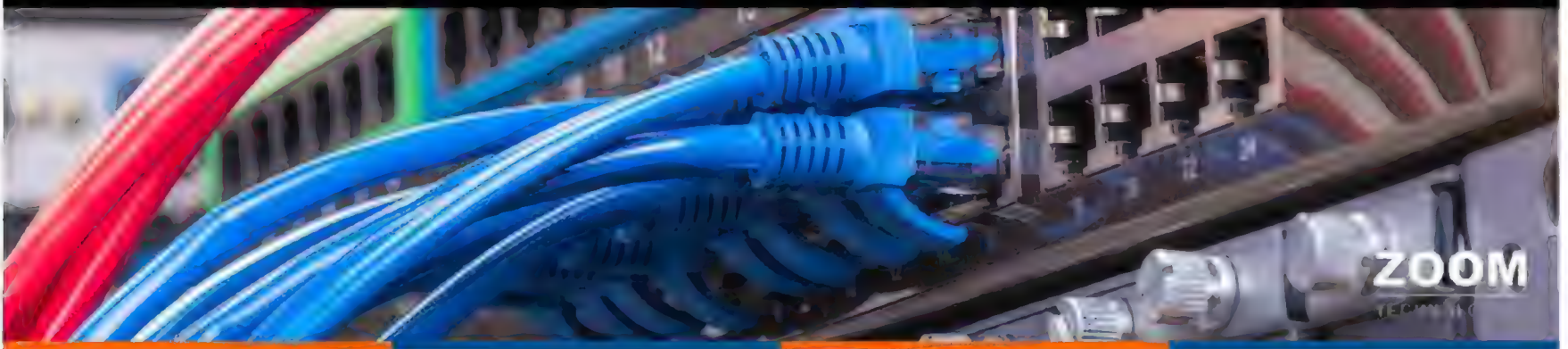
CCIE
CCNP
CCNA

- The Switch port can work like Ethernet port on Router.
- By default the port works like Layer-2 port, we can enable it to work like Layer-3 port.
- To configure it
 - SW(config-if)#no switchport
 - Assign IP and Subnet Mask
 - Router Port can be used in Routing protocols.

Zoom Technologies

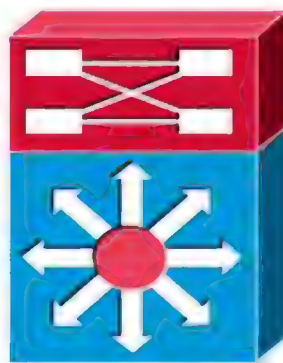


Implementing Multilayer Switching in the Network



Layer 3 Switching components

ZOOM
TECHNOLOGIES



Packet Switching:

CEF

ASIC

Layer 2 = layer 3 = layer 4

Router Processing:

Path Determination

Load Balancing

Multi Routing

Protocol Support



- Process Switching
- Fast Switching
- CEF – Cisco Express Forwarding

Zoom Technologies



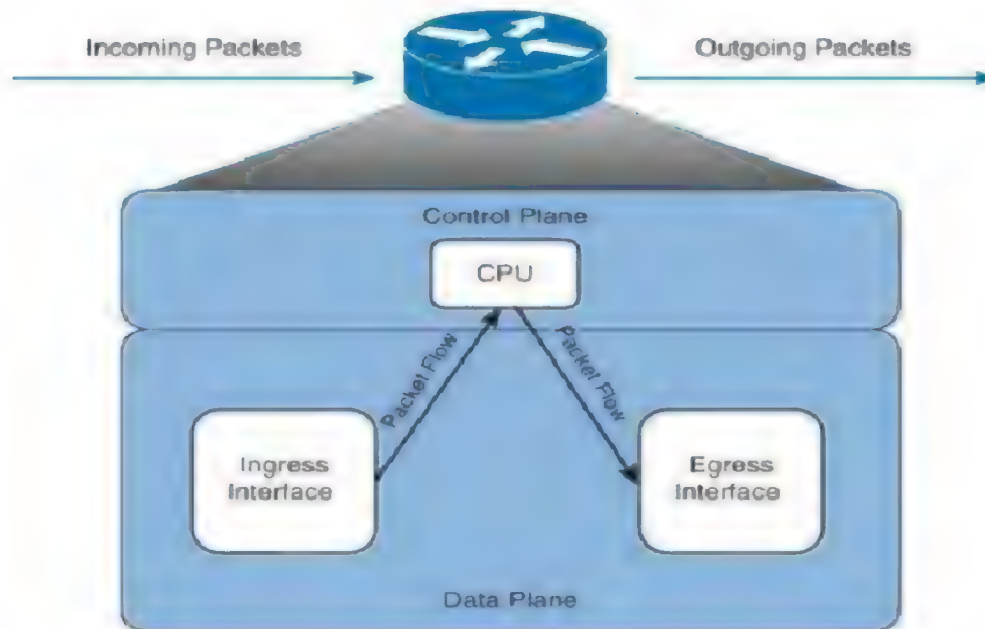
- Process Switching is the oldest method of performing packet switching
- Process switching requires the CPU to be personally involved with every forwarding decision.
- The switching decision is made on a per packet basis
- Process switching is the slowest method of packet switching

To enable Process Switching

`Router(conf-if)#no ip route-cache`

Zoom Technologies

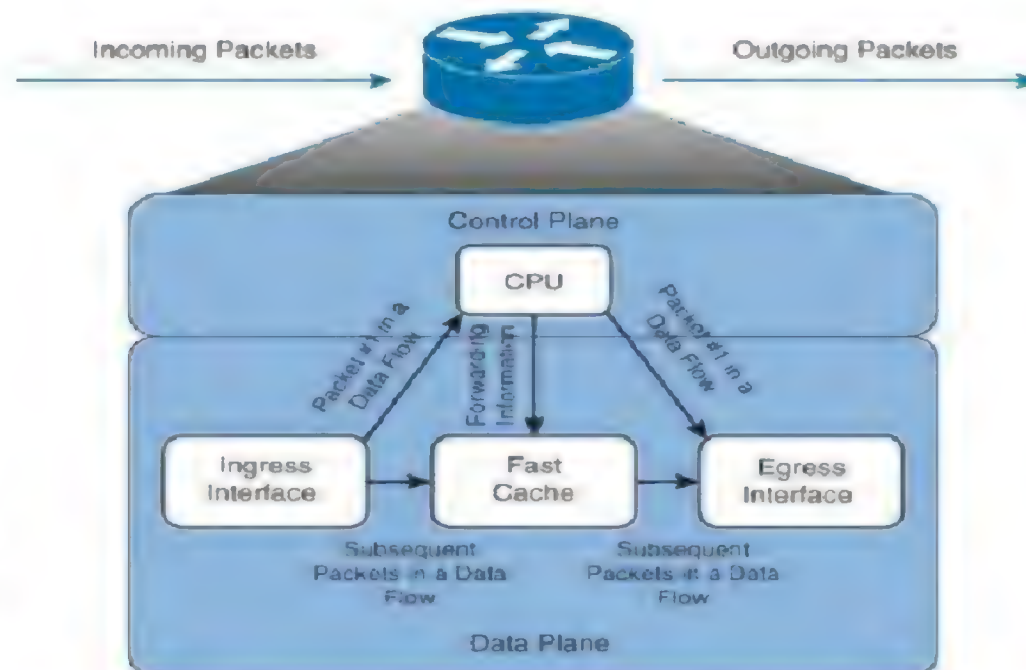




- Fast switching improves on process switching by making use of a *cache*
- The first packet to a destination is still process switched, Future packets to this destination will be switched using information from the fast cache, thus improving on the speed of this switching method.

To enable Fast Switching

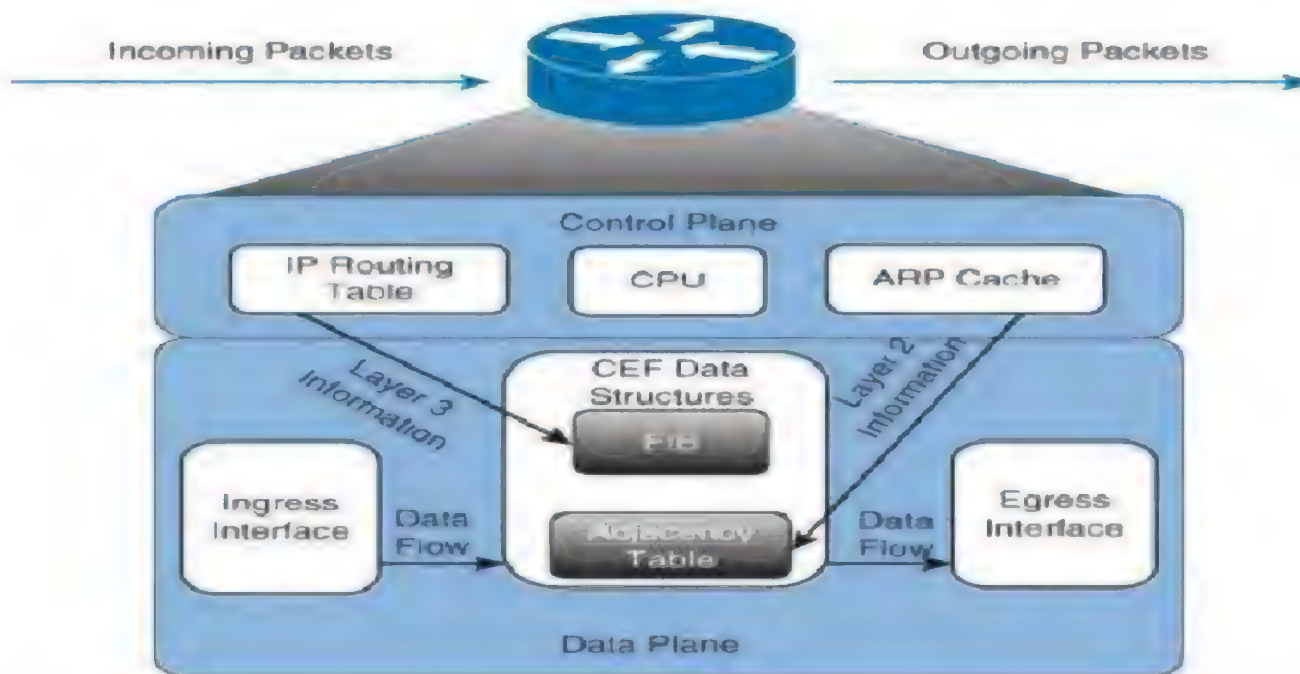
`Router(conf-if)#ip route-cache`



- CEF uses two components to perform packet switching
- Forward Information Base
- Adjacency Table
- Forward Information Base is similar to Routing Table, Adjacency Table is similar to ARP Table

- To enable CEF

Router(conf-if)#ip route-cache cef



Displaying CEF Entries in the FIB

```
Switch#show ip cef [type/slot/port number] [detail]
```

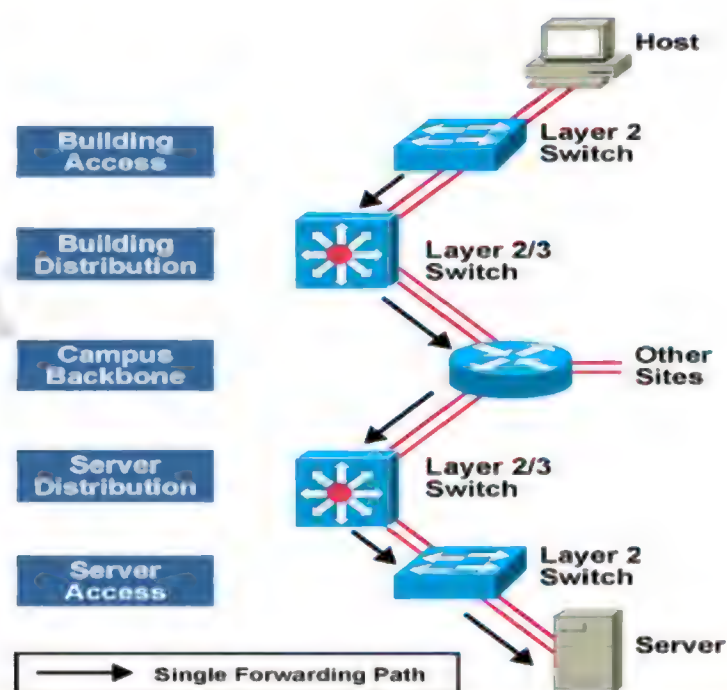
Redundancy in a Multilayer Switched Network



Single Points of Failure

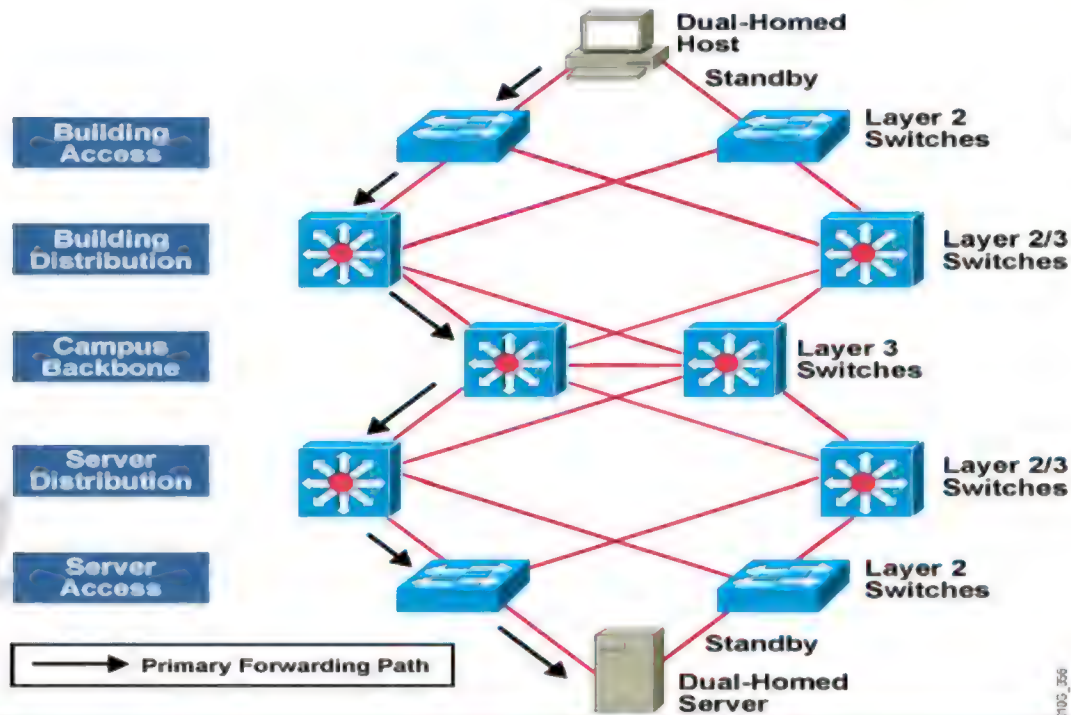
ZOOM
TECHNOLOGIES

- Redundancy within a device
- Catalyst Supervisors
- Power supplies
- Fans
- Hot-swappable Module



Redundant Switched Network with No Single Point of Failure

ZOOM
TECHNOLOGIES

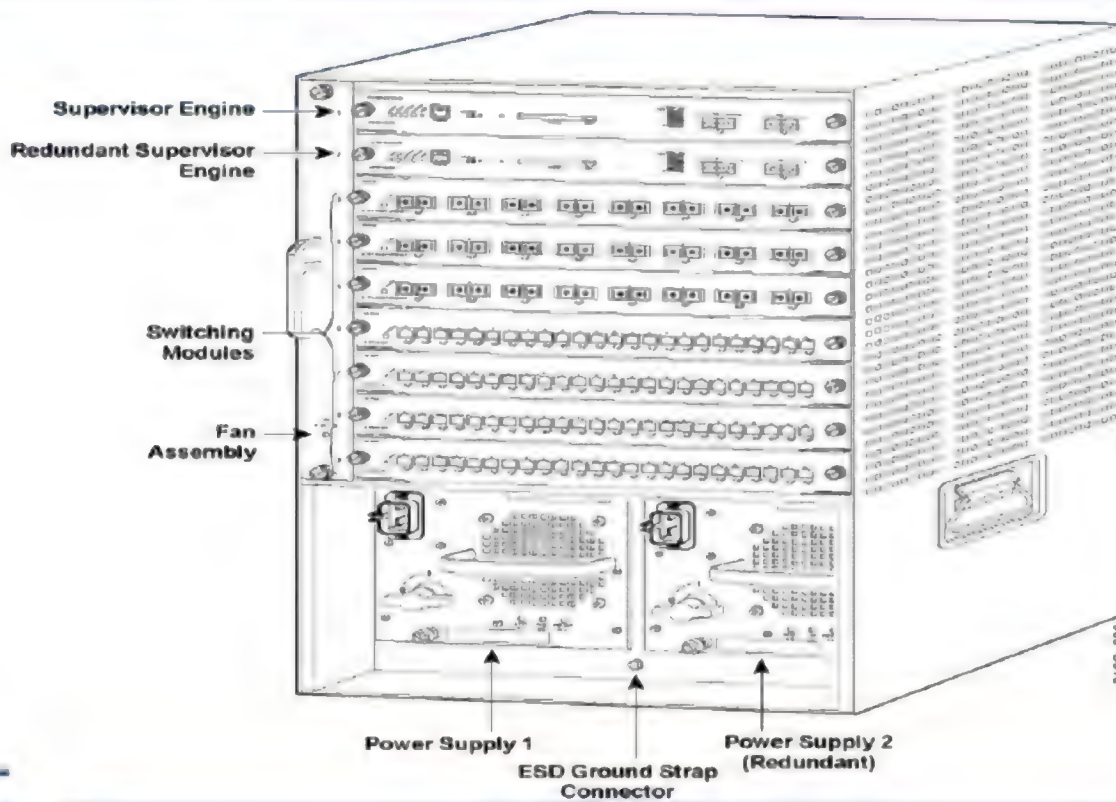


0100_356

CCIE
CCNP
CCNA

Supervisor redundancy

ZOOM
TECHNOLOGIES



0100_356

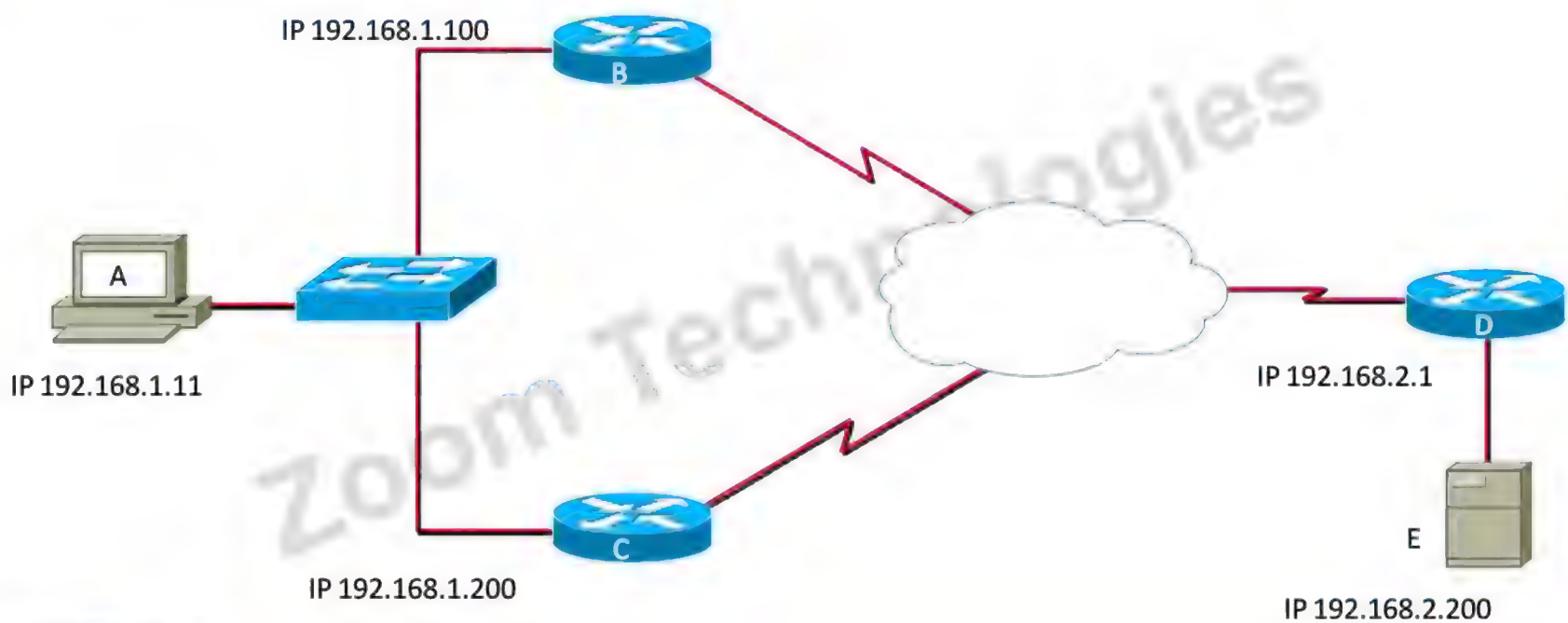
CCIE
CCNP
CCNA

Redundancy in Default Gateway

ZOOM

Problem using default Gateway

ZOOM
TECHNOLOGIES



CCIE
CCNP
CCNA



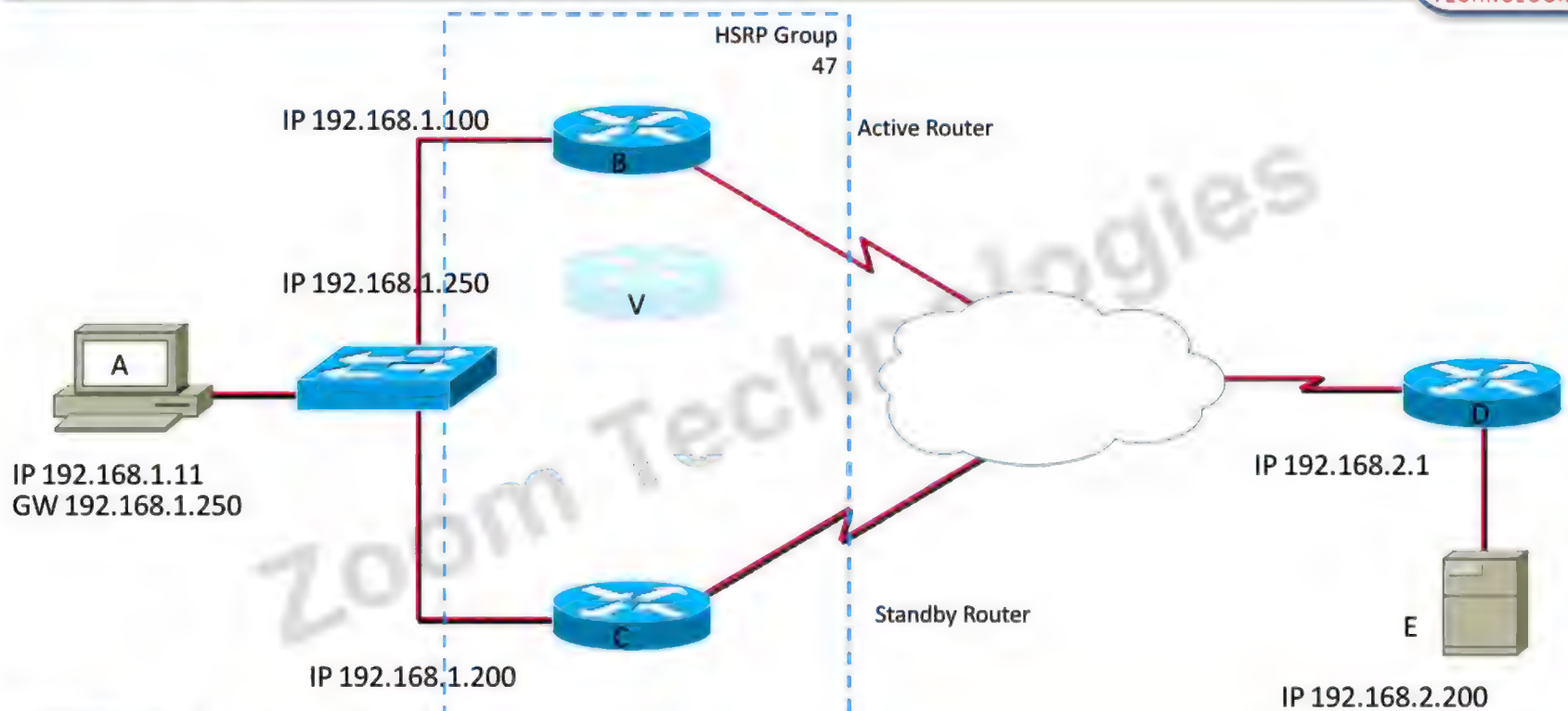
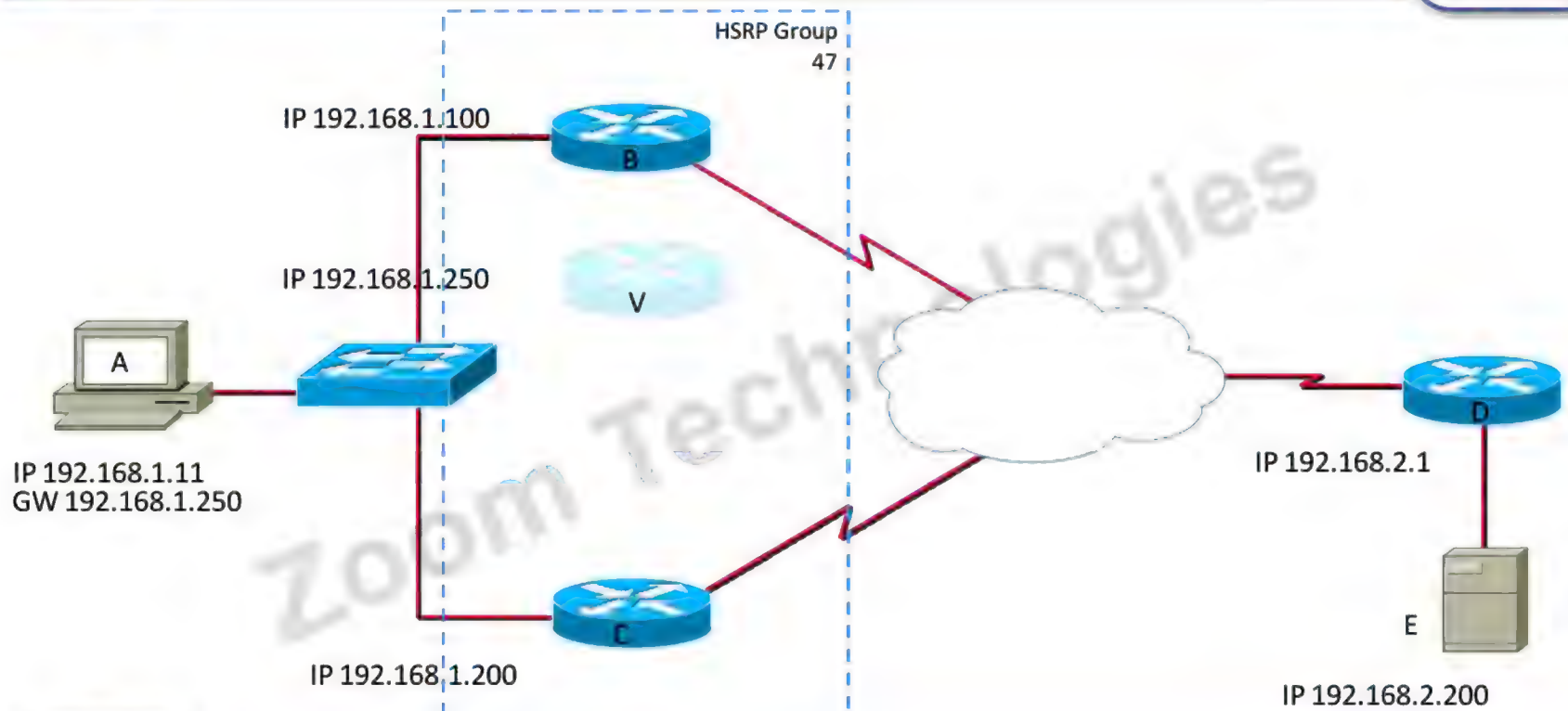
HSRP Hot Standby Routing Protocol

HSRP Hot Standby Routing Protocol

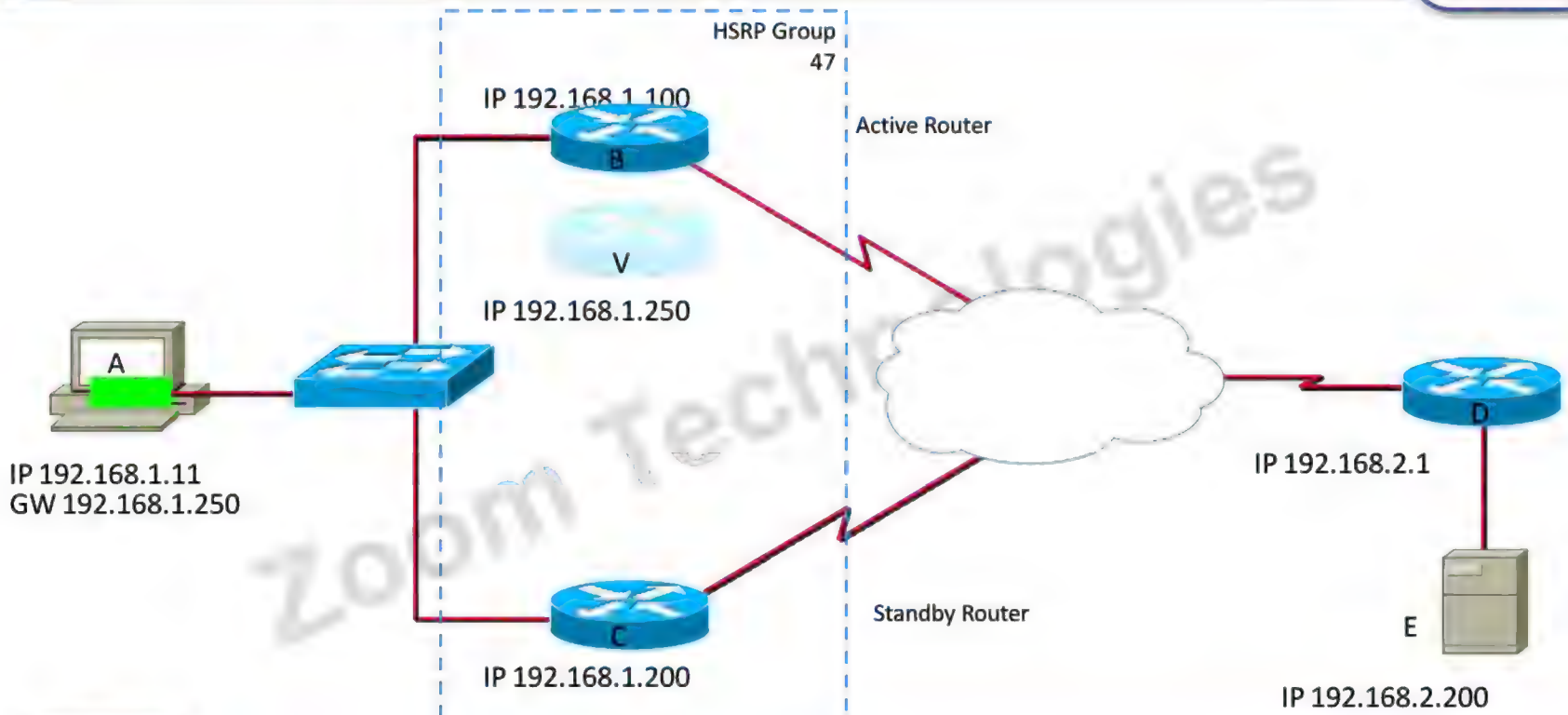
ZOOM
TECHNOLOGIES

- Cisco proprietary
- Provides Router redundancy
- Routers are grouped together, to work as one virtual router
- Group is identified by Group ID
 - Range 0 – 255 (default is 0)
 - A router can be member of multiple groups
- Two roles of Router
 - Active Router
 - Standby Router

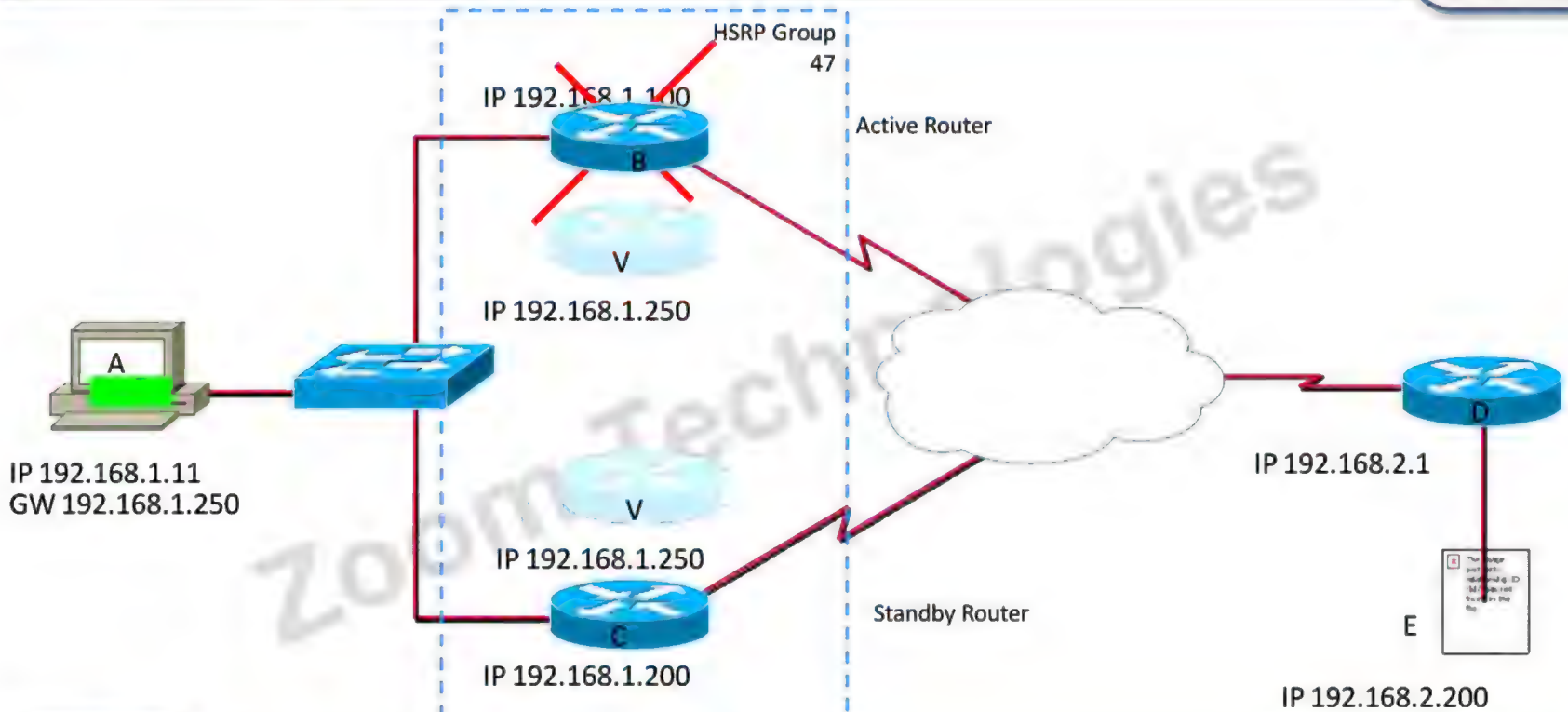


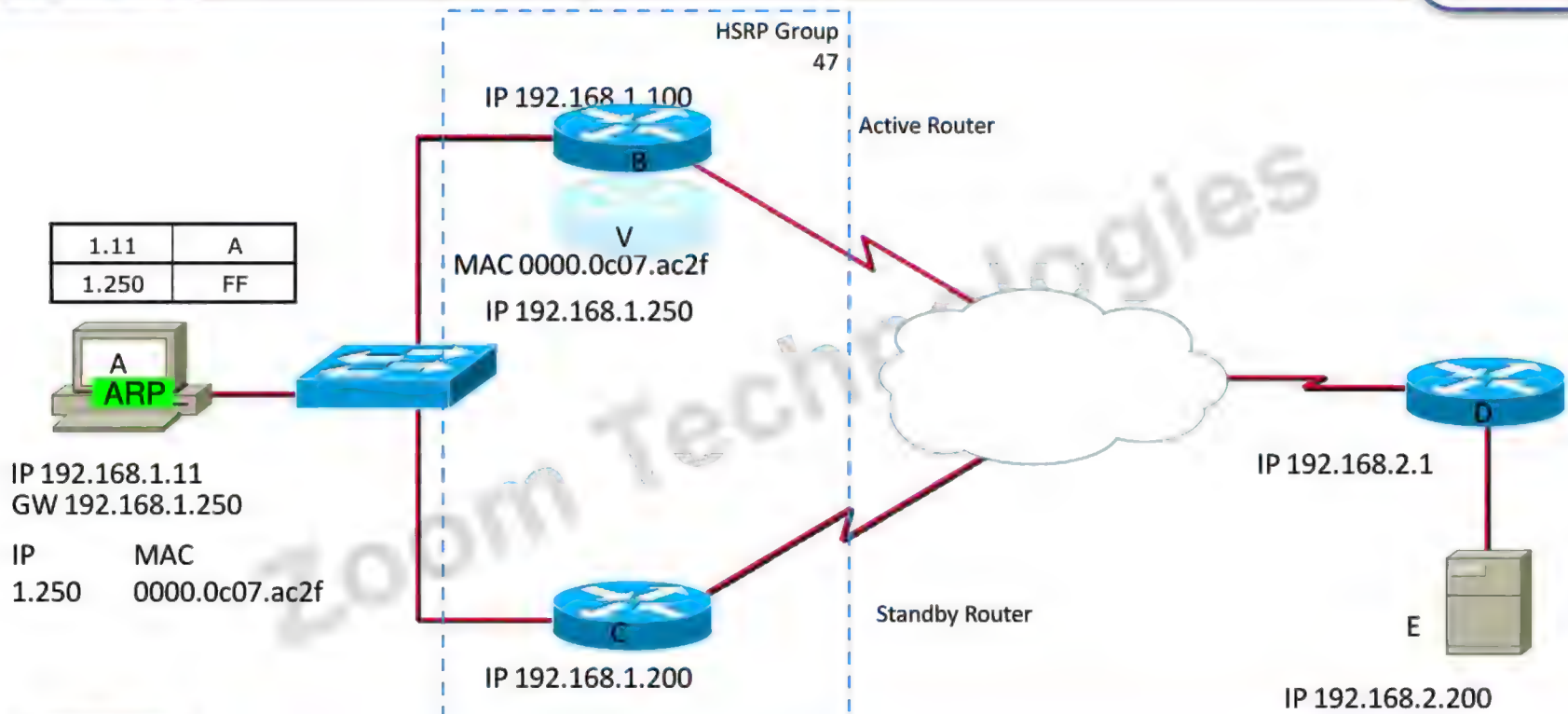


HSRP Active router Role



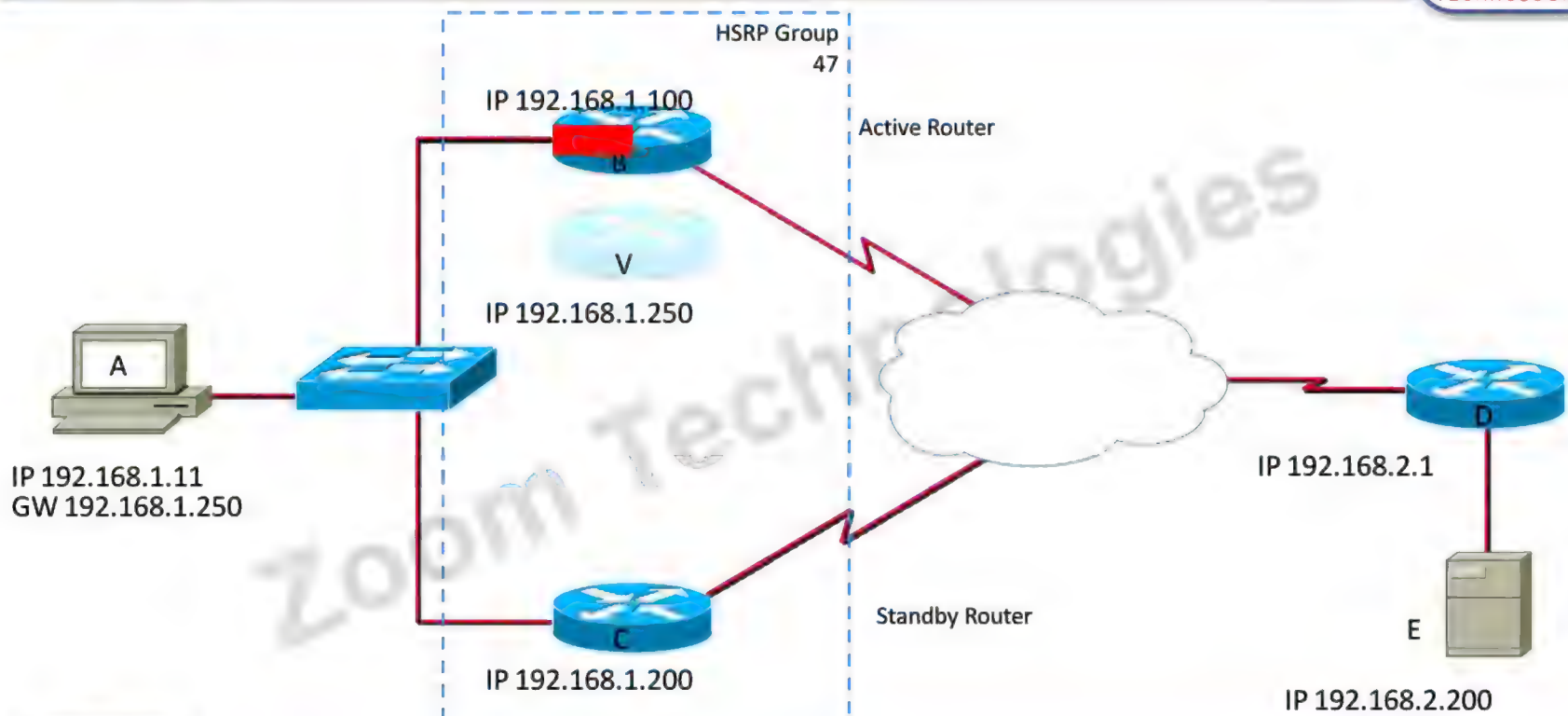
HSRP Backup Role





HSRP Elections

- HSRP is an Application Layer Protocol
- Uses UDP port 1985, multicast address 224.0.0.2 for hello message
- Hello will be sent every
 - Hello = 3 sec and hold = 10
- HSRP Election priority
 - Router with highest Priority
 - Router with highest Physical IP



To create and assign ip address in HSRP group

```
Router(config-if)#standby <Group No> ip <ip add>
```

Default priority is 100

Router with highest priority will win the elections

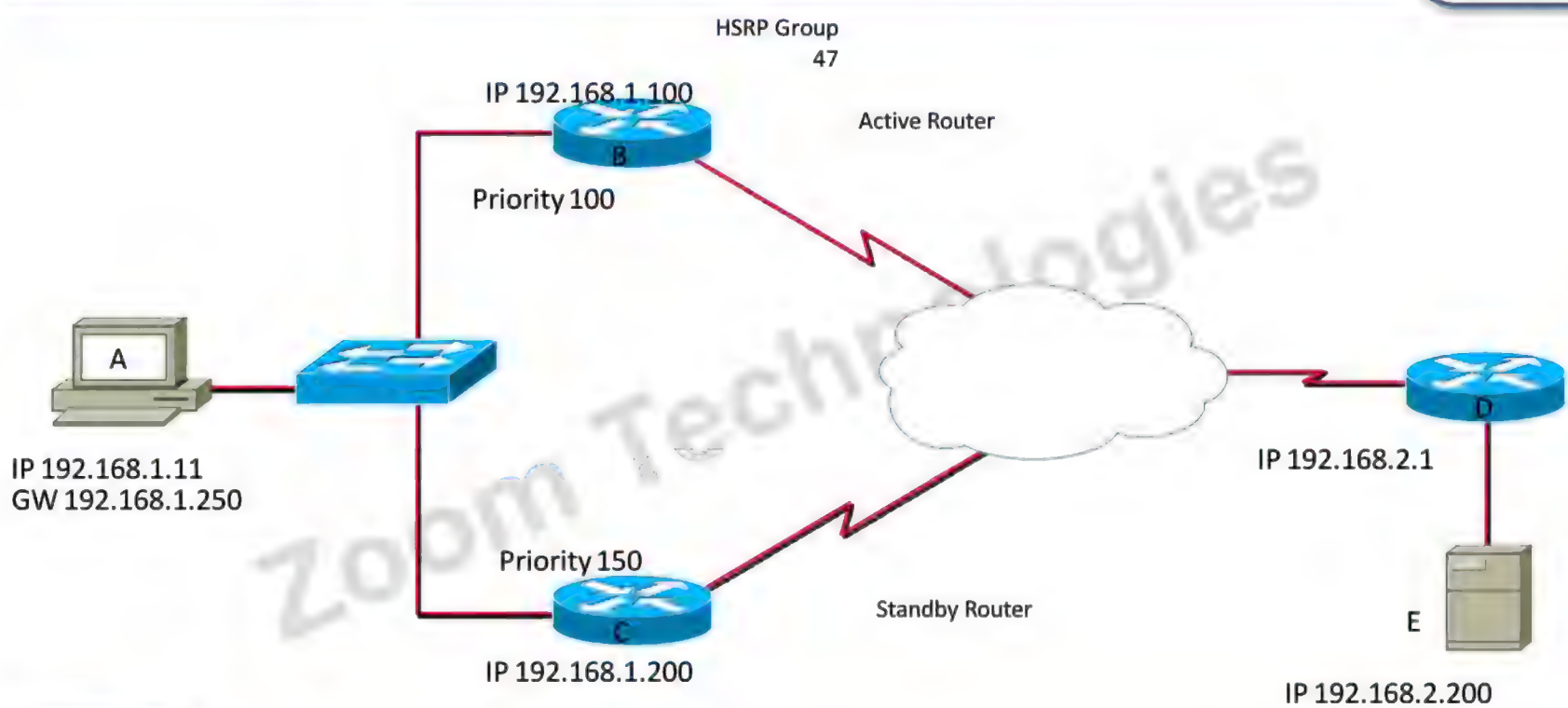
To change the Router priority

```
Router(config-if)#standby <group no> priority <pri>
```

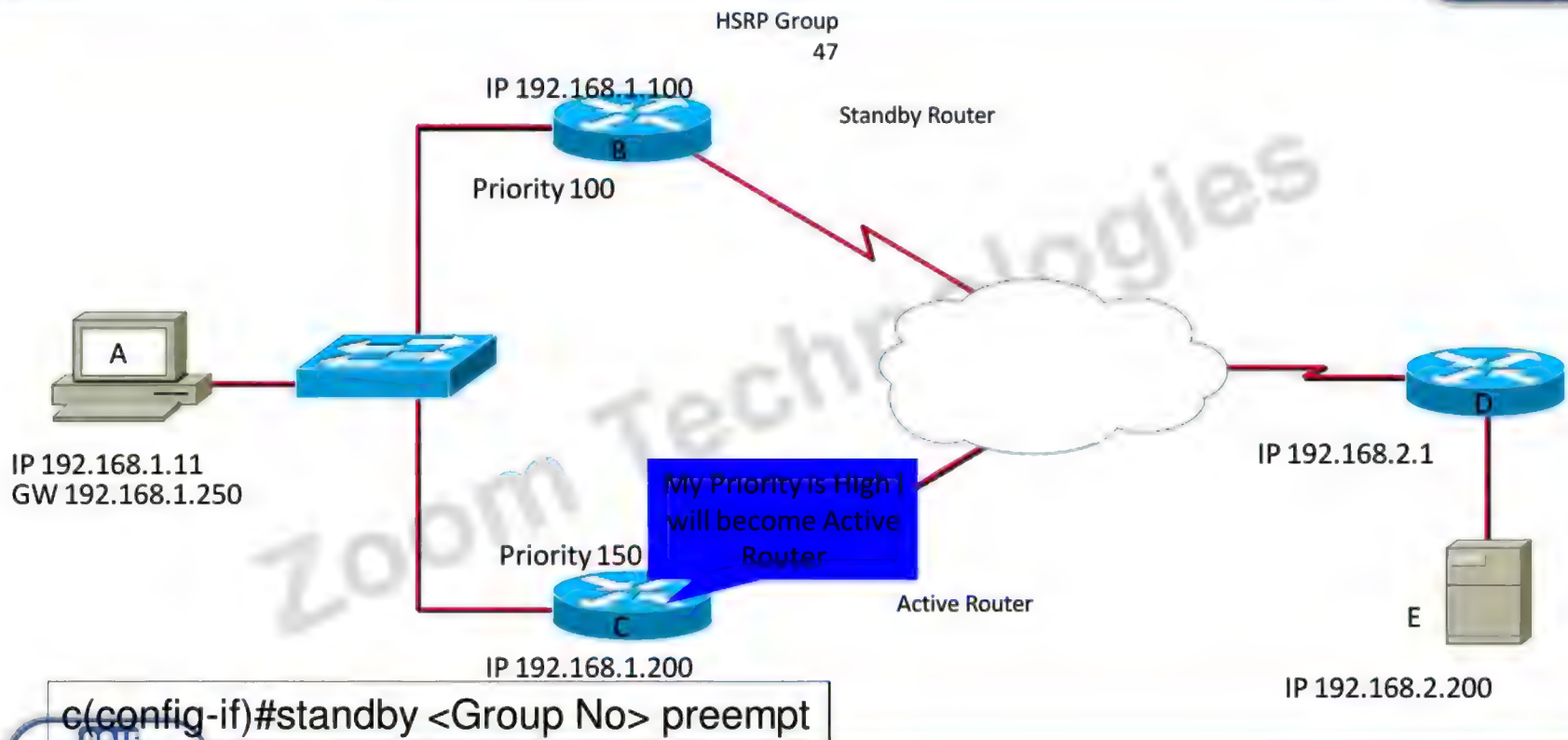
HSRP States

- Initial
- Listen
- Speak
- Standby
- Active

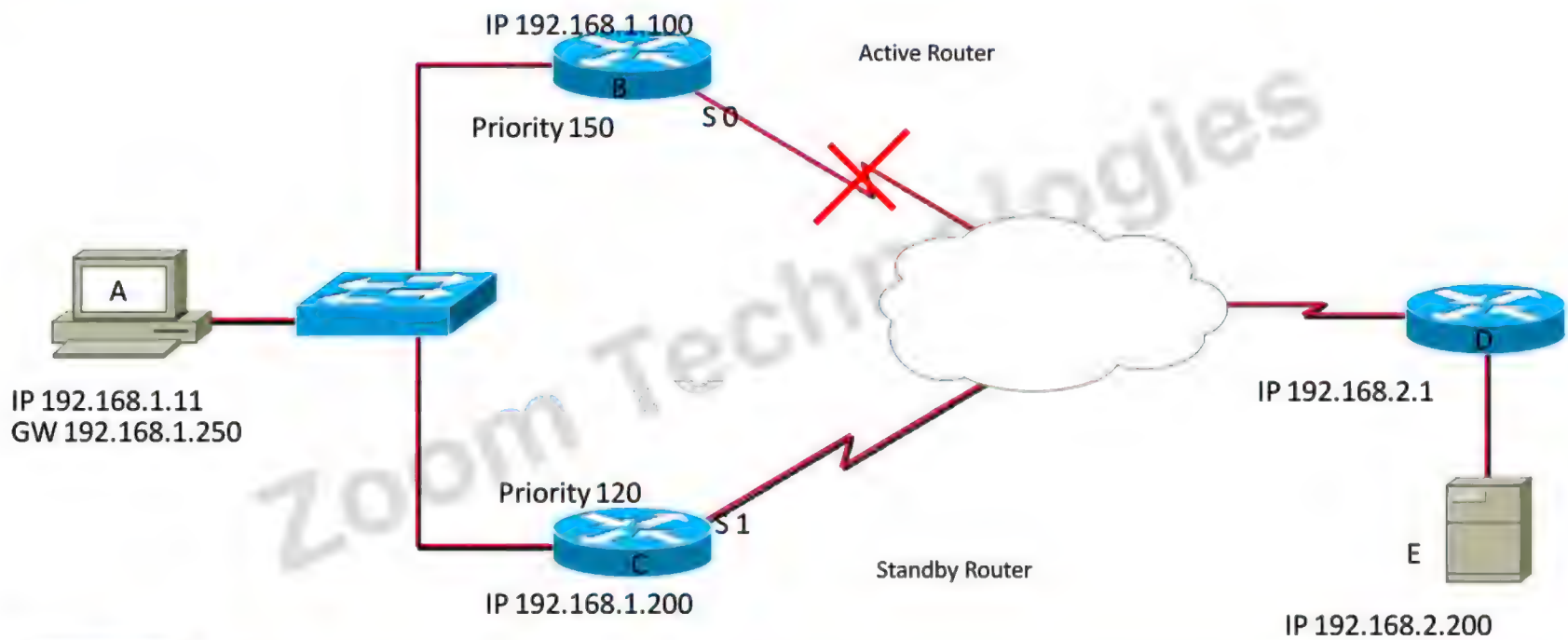
HSRP before Preempt



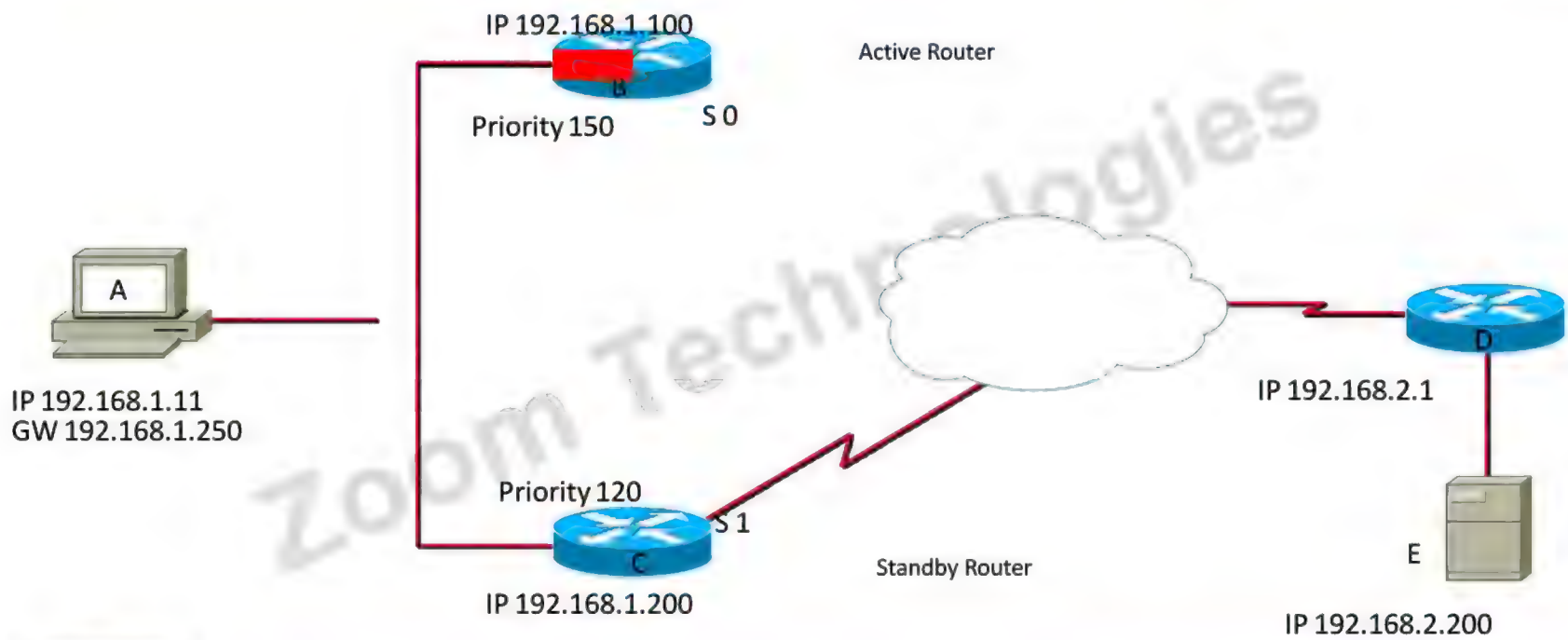
HSRP after Preempt



HSRP Interface Tracking

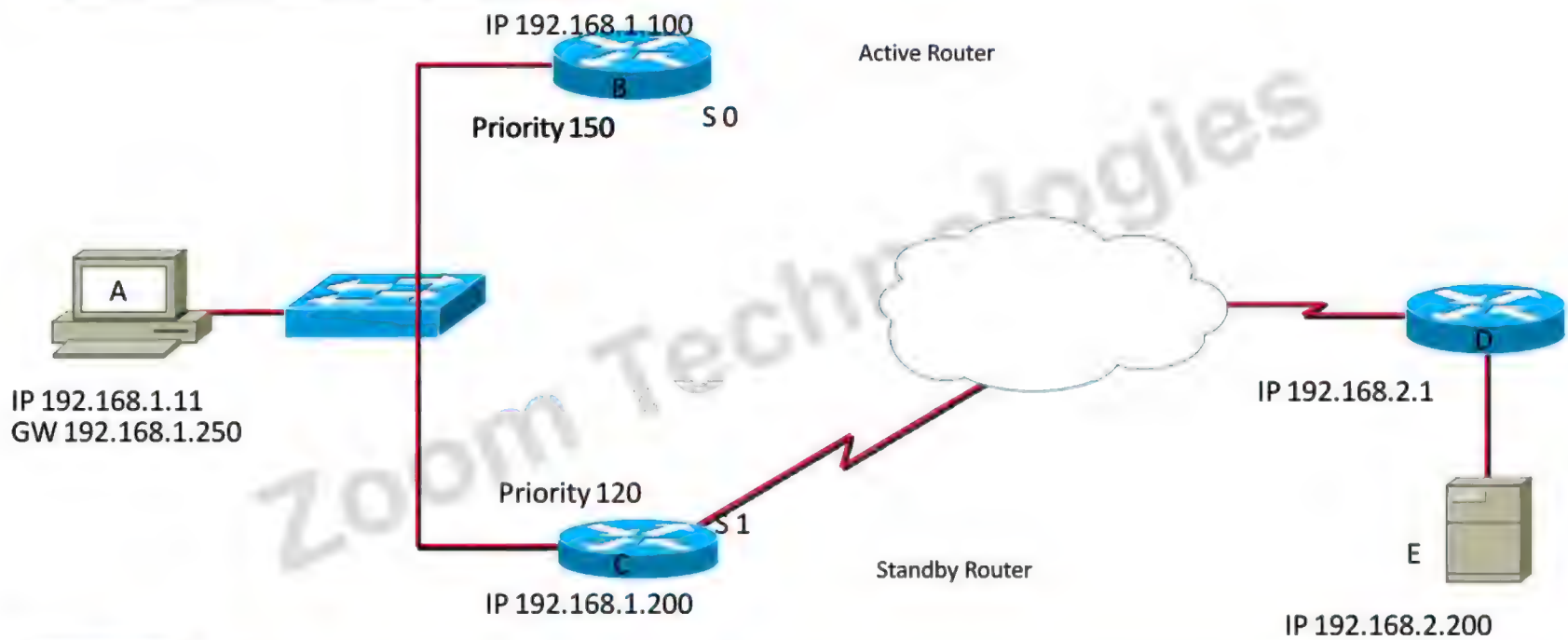


HSRP Interface Tracking



HSRP Interface Tracking

```
b(config-if)#standby <Group No> track s 0 31
```



```
Router(config-if)#standby <G No> track <int type> <no> <Priority>
```

To decrement amount of priority from HSRP

When ever interface go down

Note Preempt command is pre required on both router for this command to work



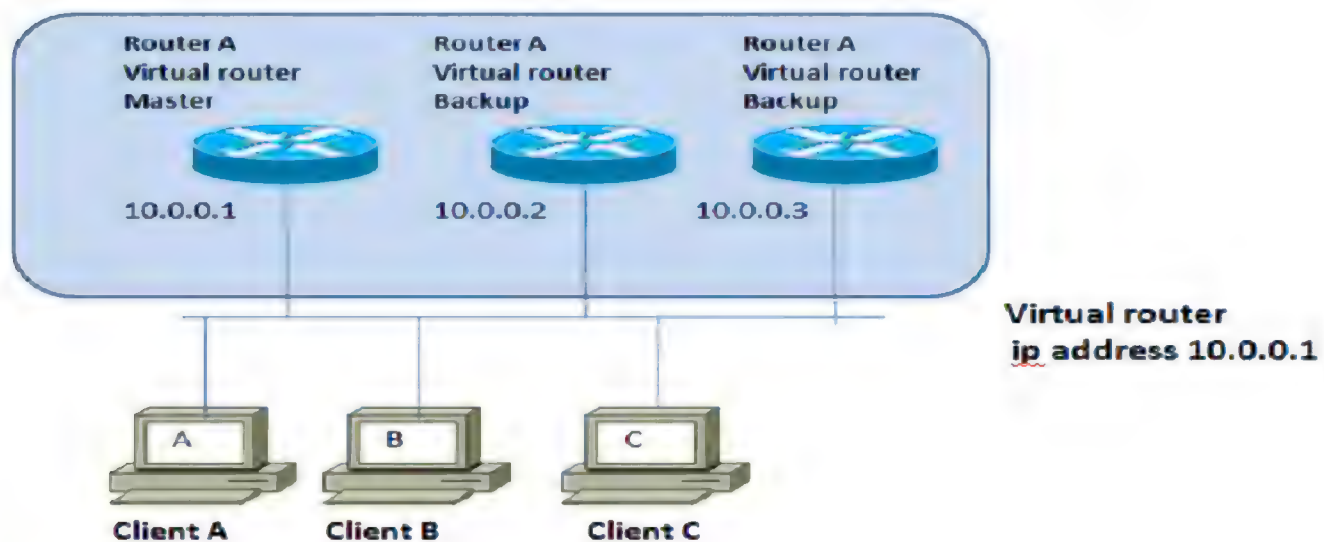
Virtual Router Redundancy Protocol



- Open Standard protocol
- Provides Router redundancy
- Routers group together to work as one virtual router
- Group is identified by Group ID
 - Range 0 – 255 (default is 0)
- Group has two types of router
 - Master router
 - Backup Router

- Master Router
 - Only one master per group
 - Actively forwards traffic coming for virtual IP
- Backup Router
 - Multiple Backup routers per Group

- VRRP is a Network Layer Protocol
- Uses 224.0.0.18 for hello
- Hello will be send only by master
 - Hello = 1 sec and hold = 3 X hello + skew timer
 - Skew = $(256 - \text{priority}) / 256$
- VRRP Election priority
 - Router with physical IP = Virtual IP
 - Router with highest Priority
 - Router with highest Physical IP



```
Router(config-if)#vrrp <G No> ip <IP Add>
```

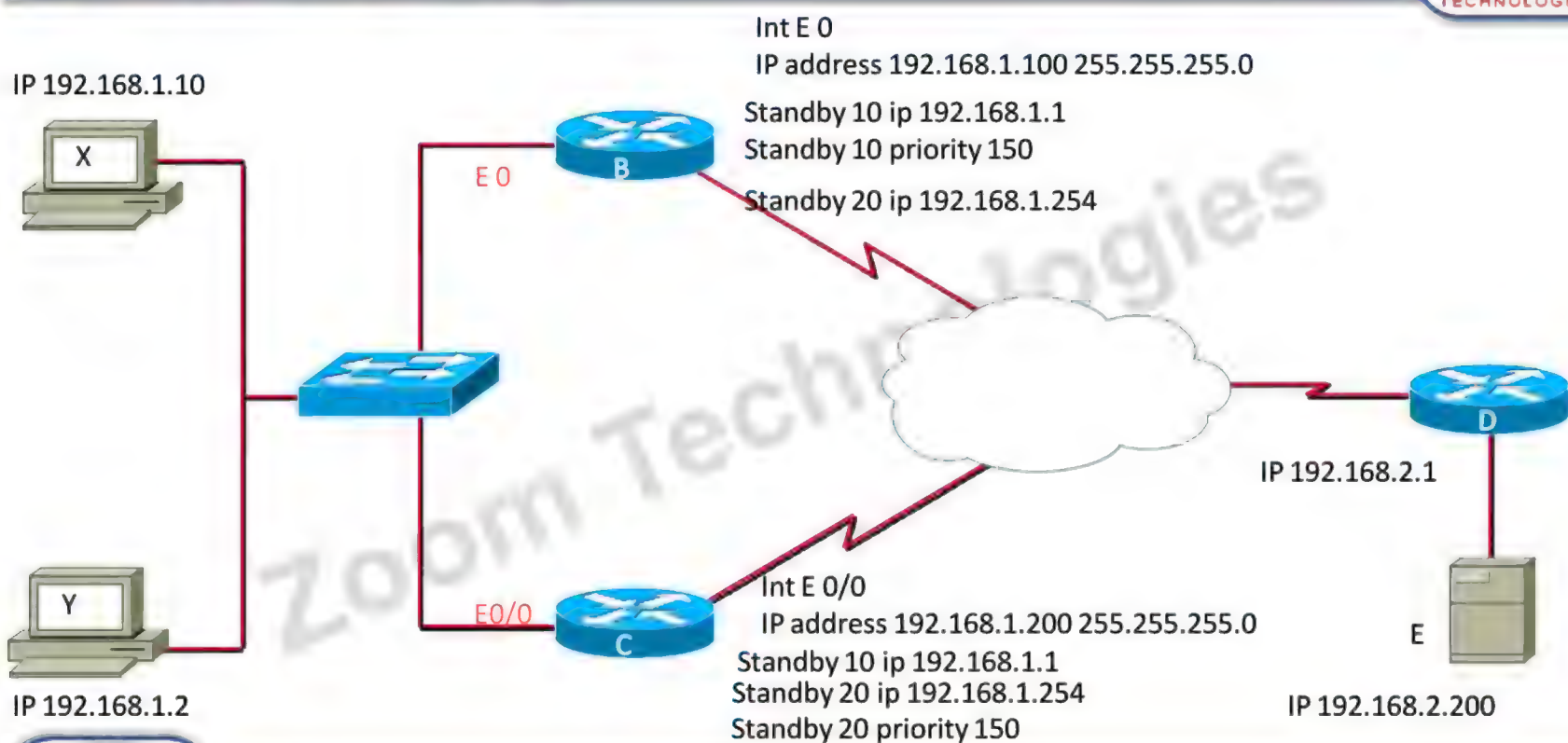
To create VRRP Group and assign IP Address

```
Router(config-if)#vrrp <G No> priority <Priority>
```

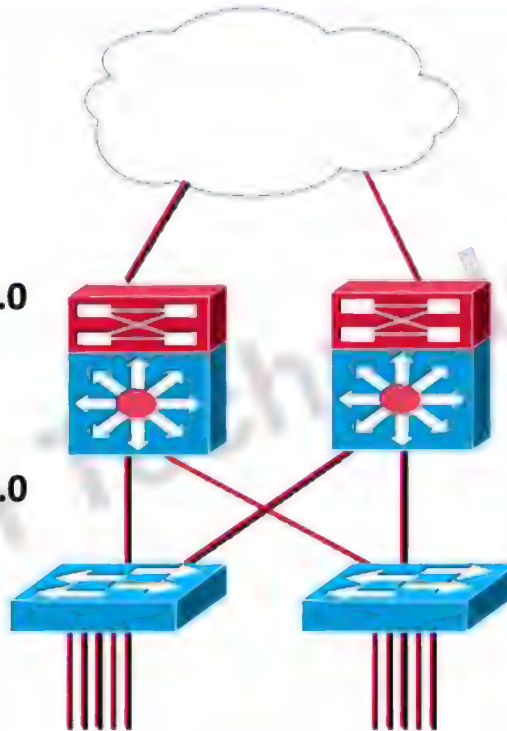
To Configure VRRP Priority for Election



Load-Balancing With HSRP/VRRP



Int VLAN 10
IP address 10.10.0.100 255.255.255.0
Standby 10 ip 10.10.0.1
Standby 10 priority 150
Int VLAN 20
IP address 10.20.0.100 255.255.255.0
Standby 20 ip 10.20.0.1



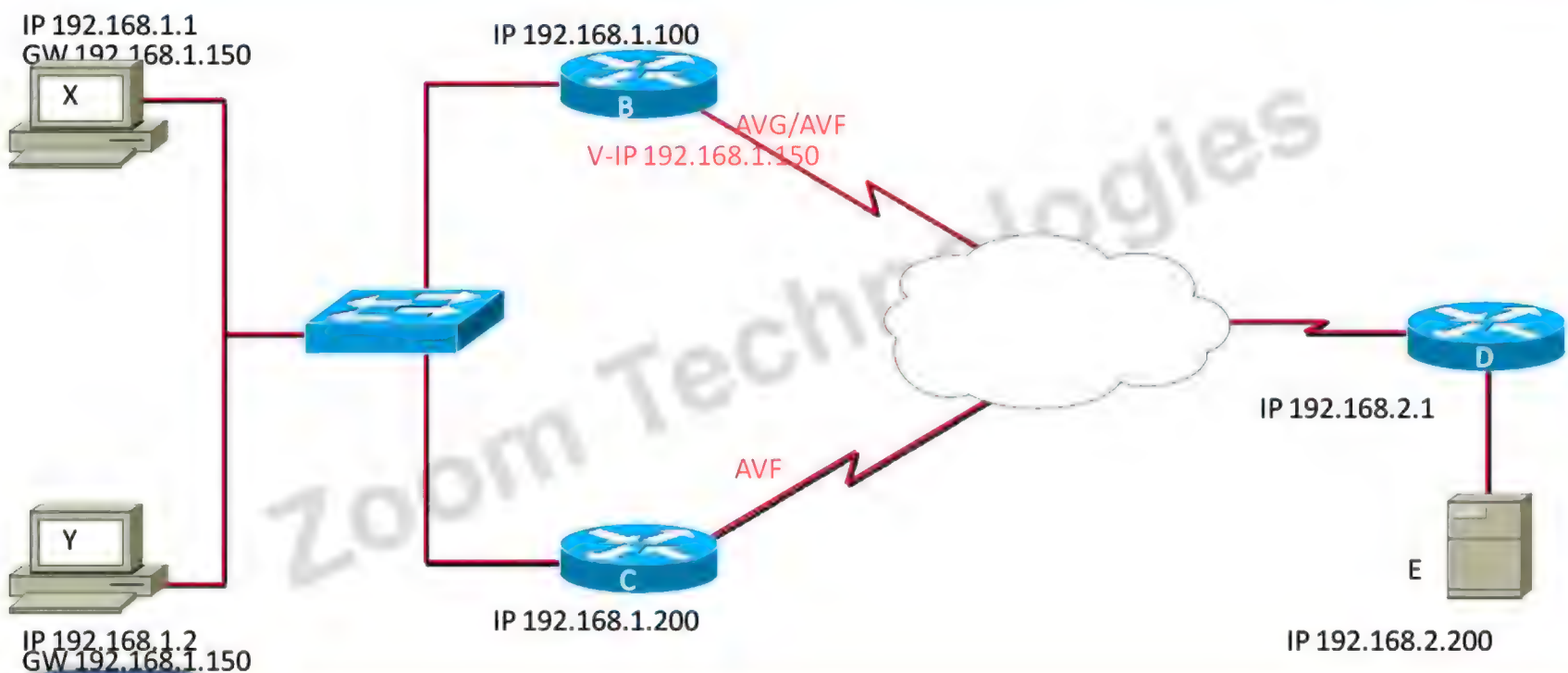
Int VLAN 10
IP address 10.10.0.200 255.255.255.0
Standby 10 ip 10.10.0.1
Int VLAN 20
IP address 10.20.0.200 255.255.255.0
Standby 20 ip 10.20.0.1
Standby 20 priority 150

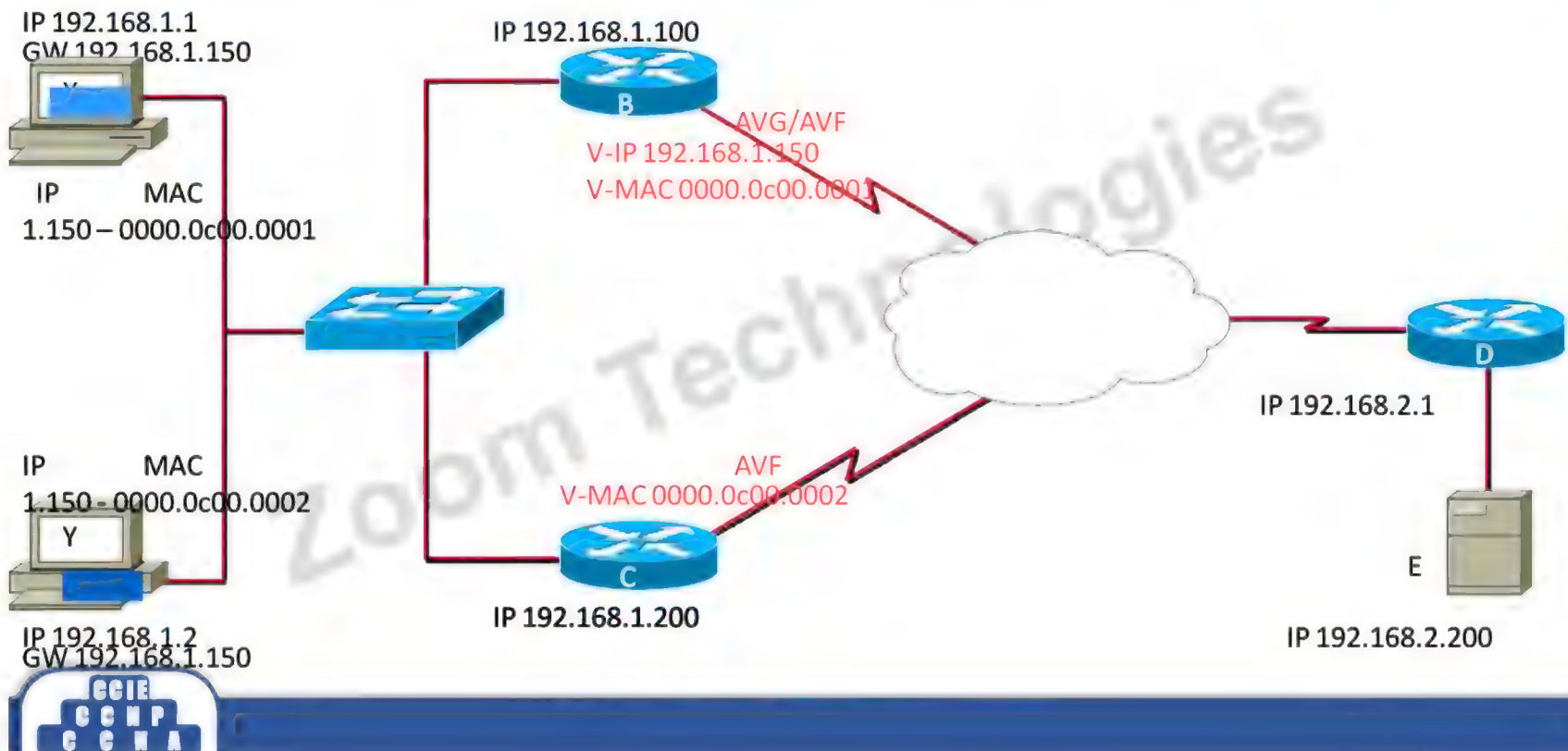
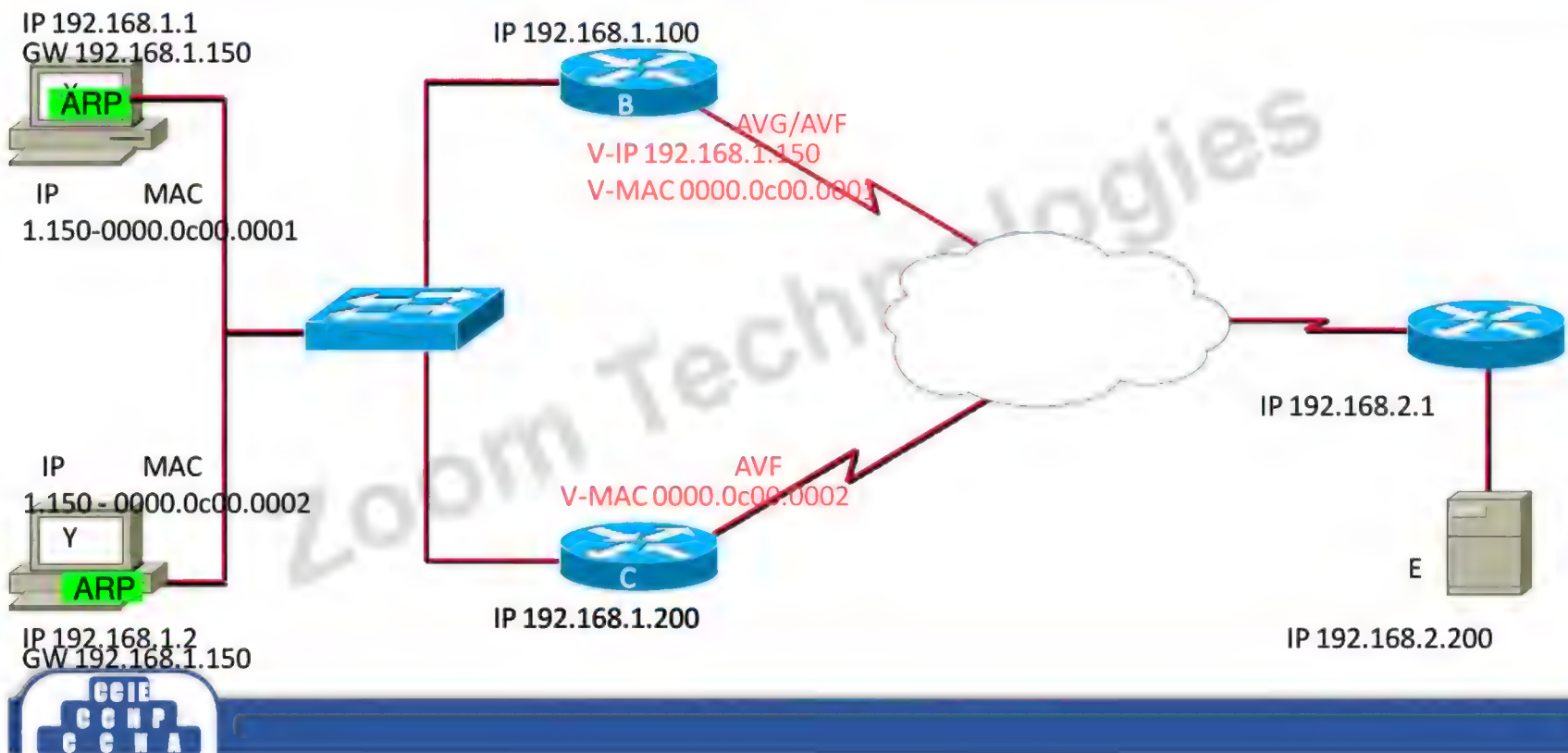
Gateway Load Balancing protocol

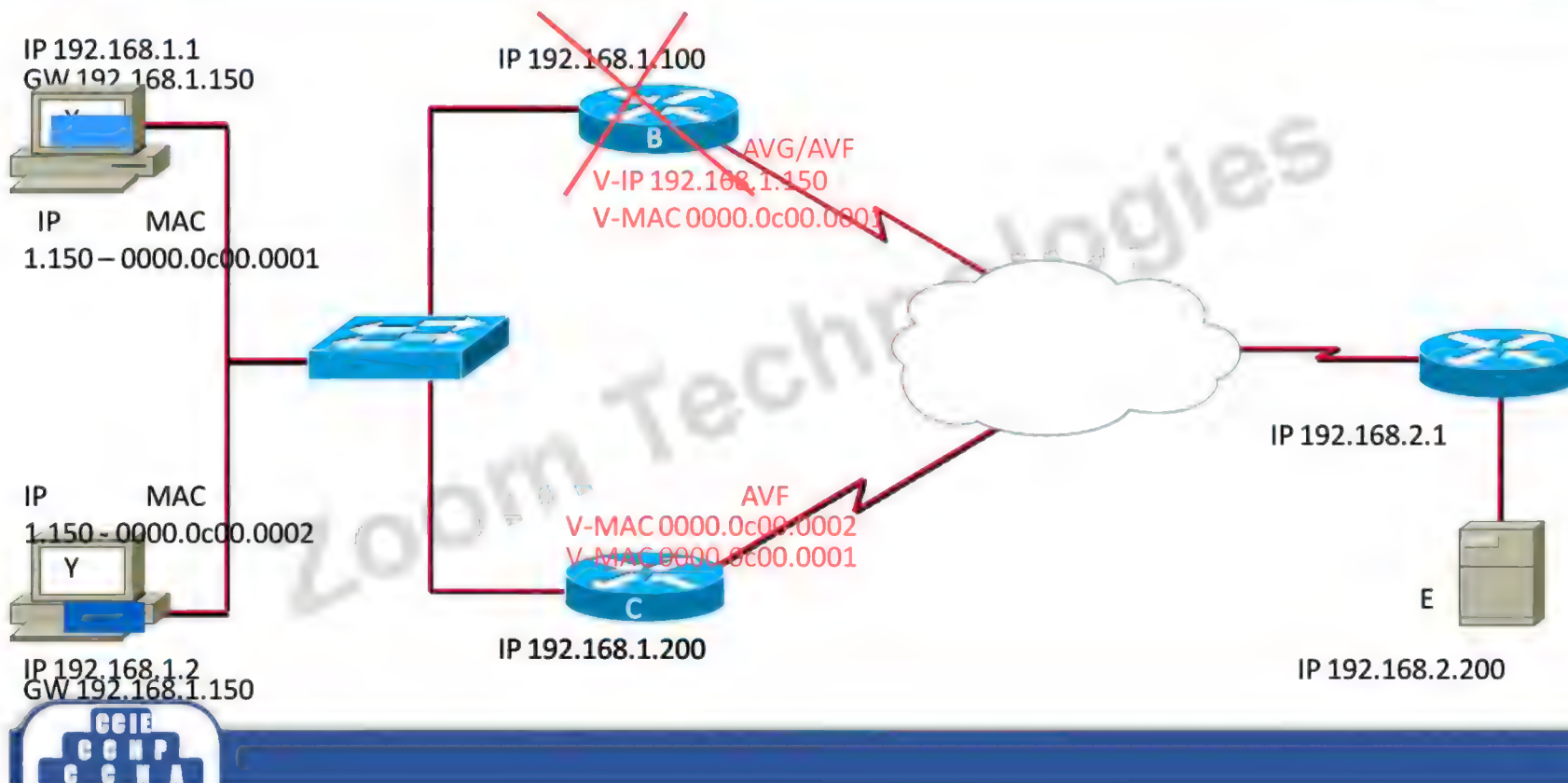
- Cisco proprietary protocol
- Provides Router redundancy with load balancing
- Routers group together to work as one virtual router
- Group is identified by Group ID
 - Range 0 – 1024 (default is 0)
- Group have two type of router
 - AVG
 - AVF

- AVG
 - Active Virtual Gateway
 - Reply for ARP coming for Virtual IP
 - Divides load among AVF
 - One Per group
- AVF
 - Active Virtual Forwarder
 - Forwards user traffic coming for Virtual MAC
 - There can be up to four forwarder per group

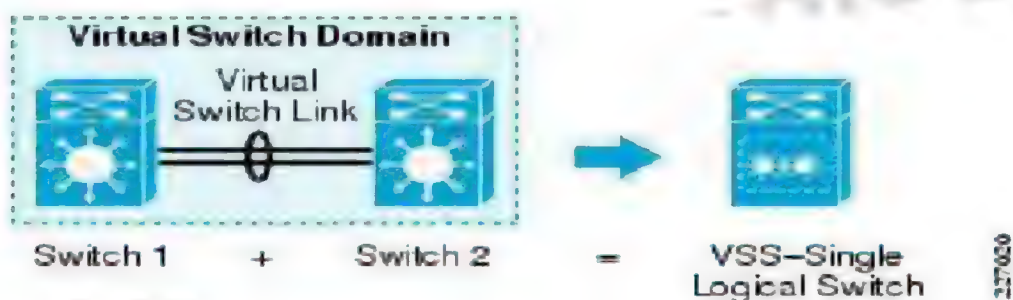
- GLBP have two elections per Group
 - Active Virtual Gateway
 - Router with Highest Priority (default 100)
 - Router with Highest Physical IP
 - Only one AVG Per group
 - Election are non-preemptive
 - Active Virtual Forwarder
 - Router with Highest weight (default 100)
 - Router with Highest Physical IP
 - Up to four AVF Per group
 - Election are preemptive



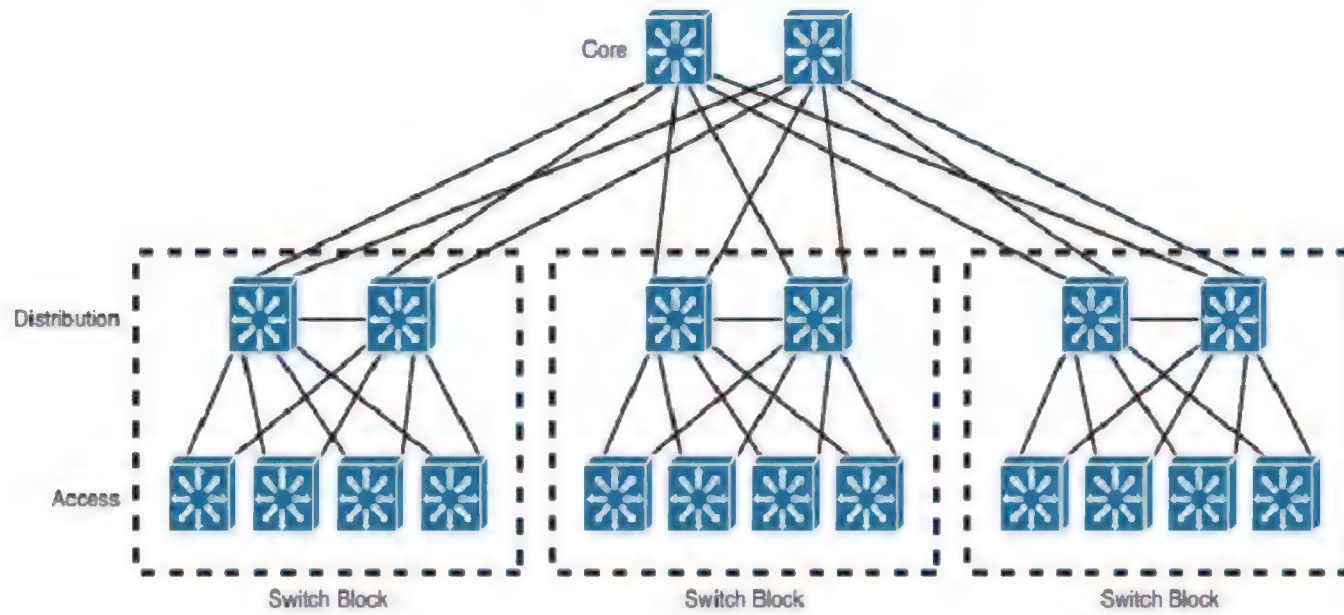




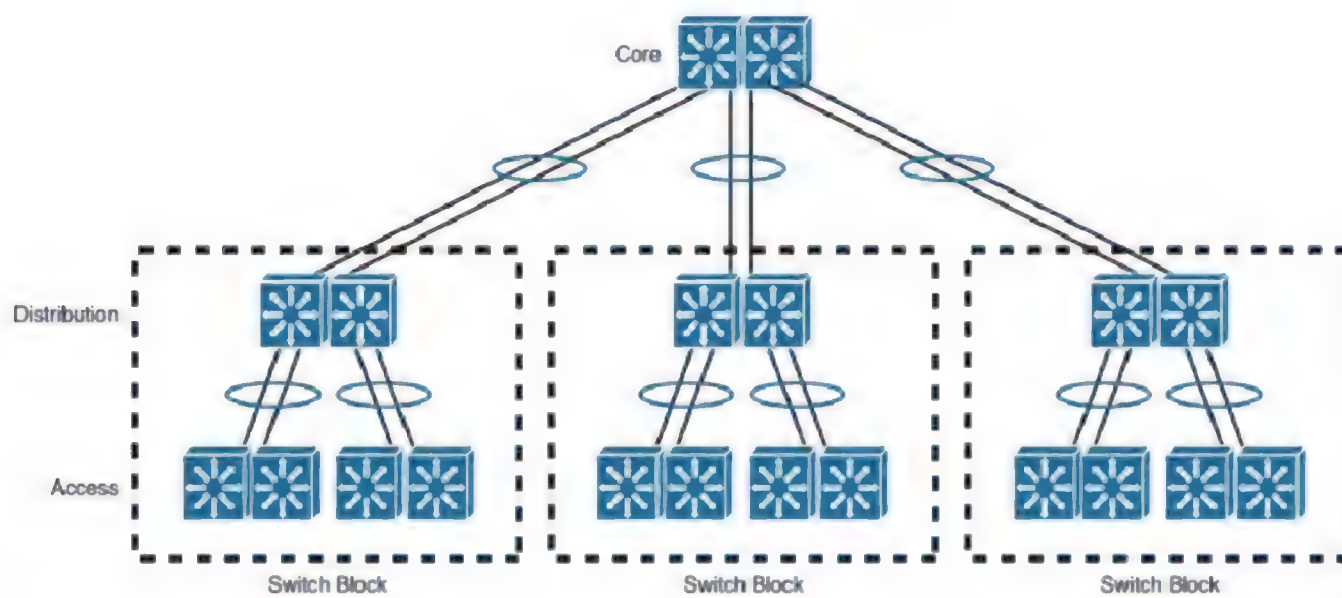
- The Virtual Switching System (VSS) allows two Cisco Catalyst 6500 or 4500 to combine together as one mega switch
- Other devices will see the VSS configured 6500 as a single device
- Two switches will be combined by using a special link called a Virtual Switch Link (VSL).

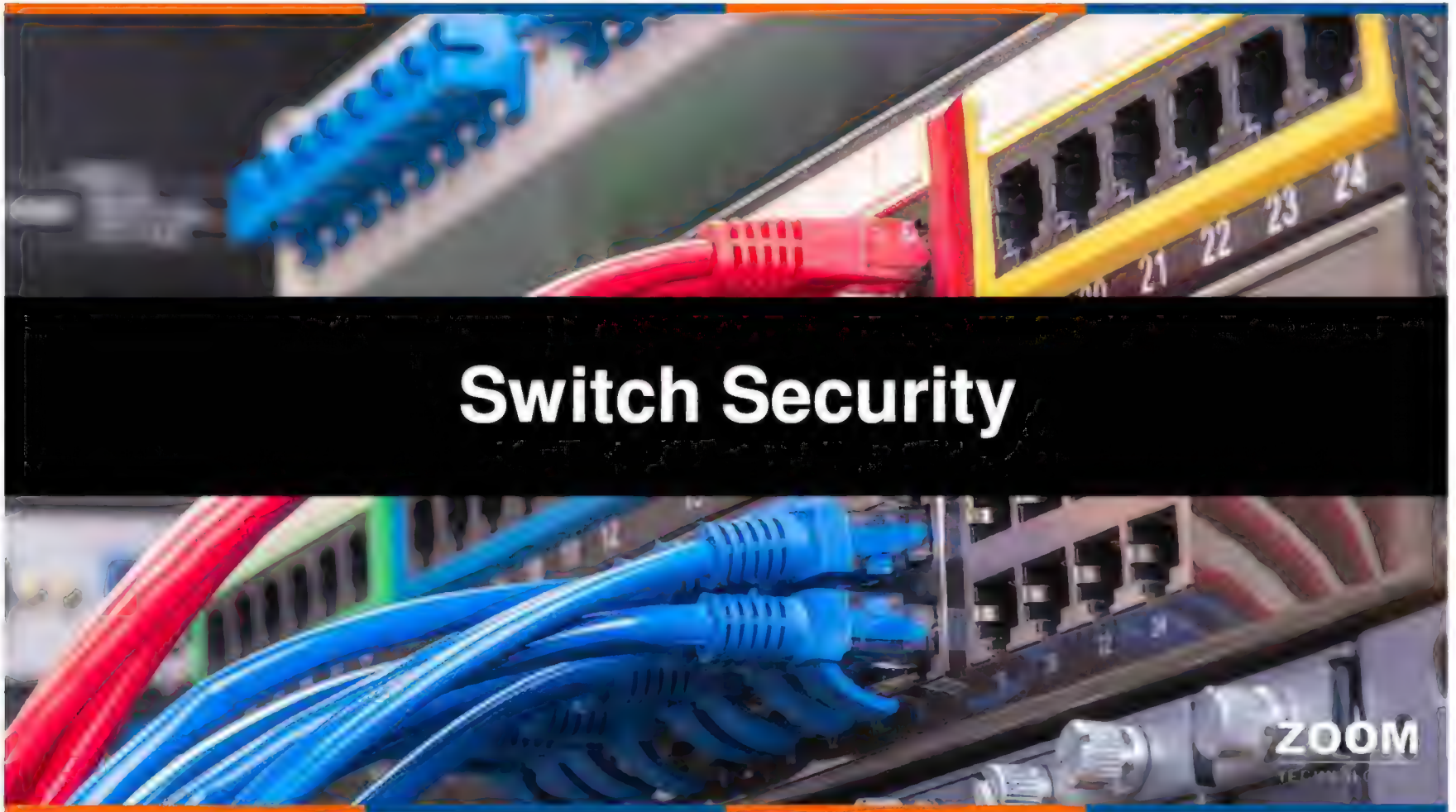


Without VSS



With VSS





Recommended Switch Security

ZOOM
TECHNOLOGIES

- **Configure Secure Passwords**
- **Configure basic ACLs**
- **Secure physical access to the console**
- **Secure access to VTYS**
- **Configure system warning banners**
- **Disable unneeded services**
- **SSH**



- **Authentication**
 - Verifies a user's identify
- **Authorization**
 - Specifies the permitted tasks for the user
- **Accounting**
 - Provides billing, auditing and monitoring



- **Authentication provides the method of identifying users.**
The most common method of authentication is username/password.
- **Authorization provides a method of controlling access to what a user can do.**
Authorization is usually tied to a policy, profile or group.
- **Accounting provides a method for collecting and sending security server information used for billing, auditing, and reporting.**
Accounting collects data as to what a user did once logged in.





- Zoom Technologies

To enable AAA

- Switch(conf)#aaa new-model
- Switch(conf)#aaa authentication login default group radius
- Switch(conf)#radius-server host 192.168.0.1 key zoom123
- Switch(conf)#line vty 0 4
- Switch(conf-line)#login authentication default



Switch Attack Categories

- **MAC Flooding Attack**

MAC Flooding attack is a type of attack where switch port will receive large number of Frames with Fake MAC addresses.

- **VLAN Hopping Attack**

VLAN hopping (virtual local area network hopping) is a method of attacking a network by sending packets to a port that is not normally accessible from a given end system.

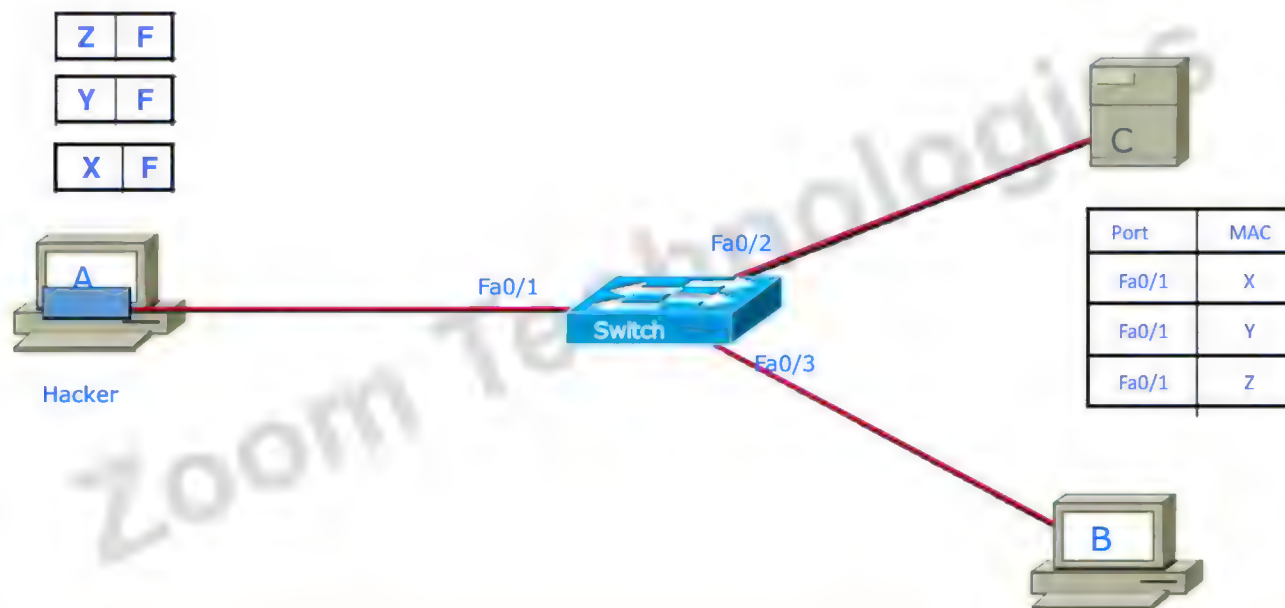
- **Spoofing Attacks**

Switch spoofing can occur when the switch port an attacker connects to is either in trunking mode or in DTP auto-negotiation mode



MAC Flooding Attacks

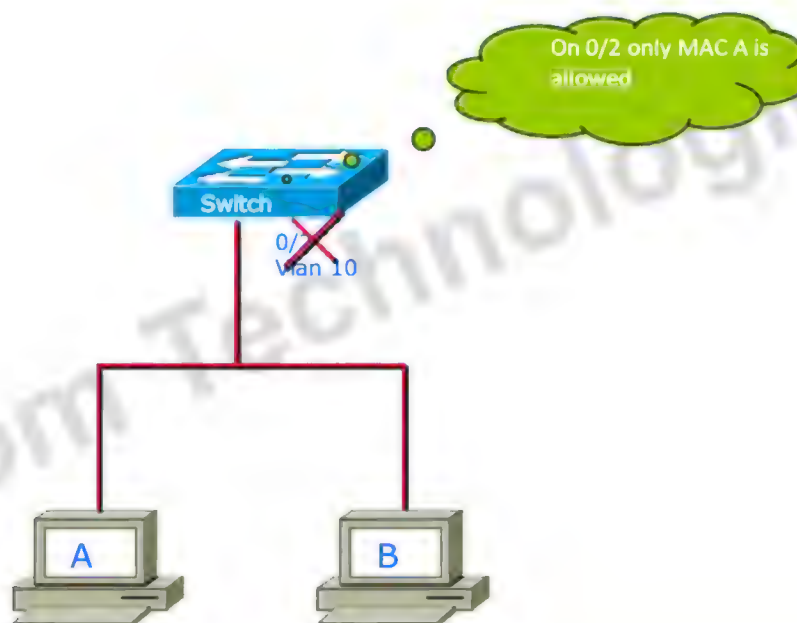
ZOOM
TECHNOLOGIES



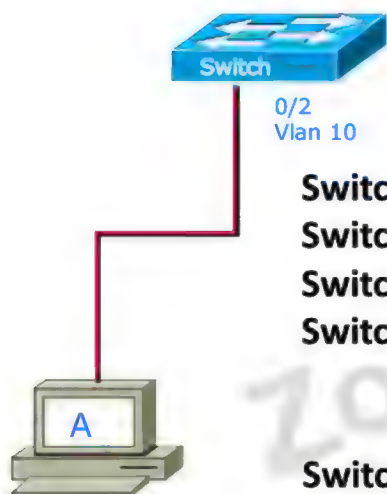
CCIE
CCNP
CCNA

Network Access Port Security

ZOOM
TECHNOLOGIES



CCIE
CCNP
CCNA



```
Switch(c)#interface fa 0/2
Switch(c-if)#switchport port-security
Switch(c-if)#switchport port-security max 1
Switch(c-if)#switchport port-security mac-address
0000.0000.000a
```

```
Switch(c-if)# switchport port-security violation
<shutdown | protect | restrict>
```

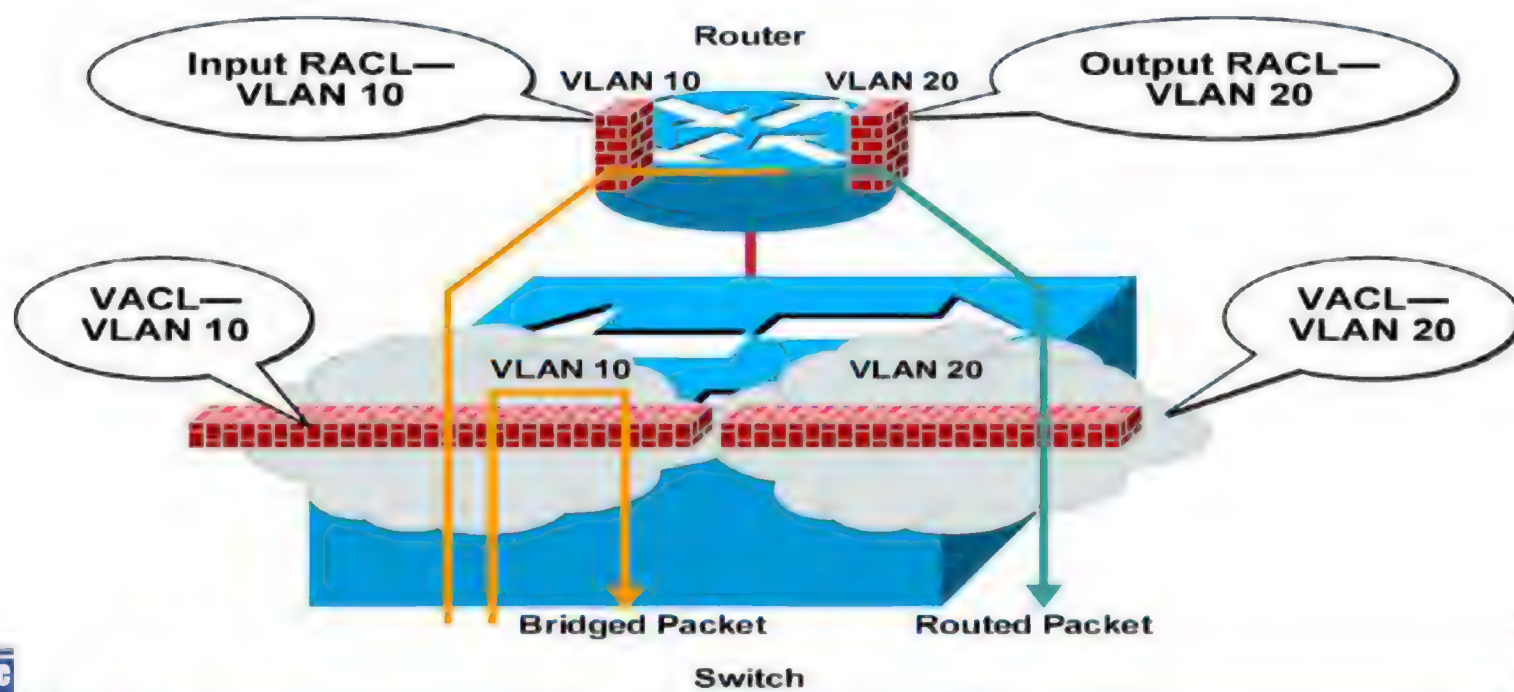
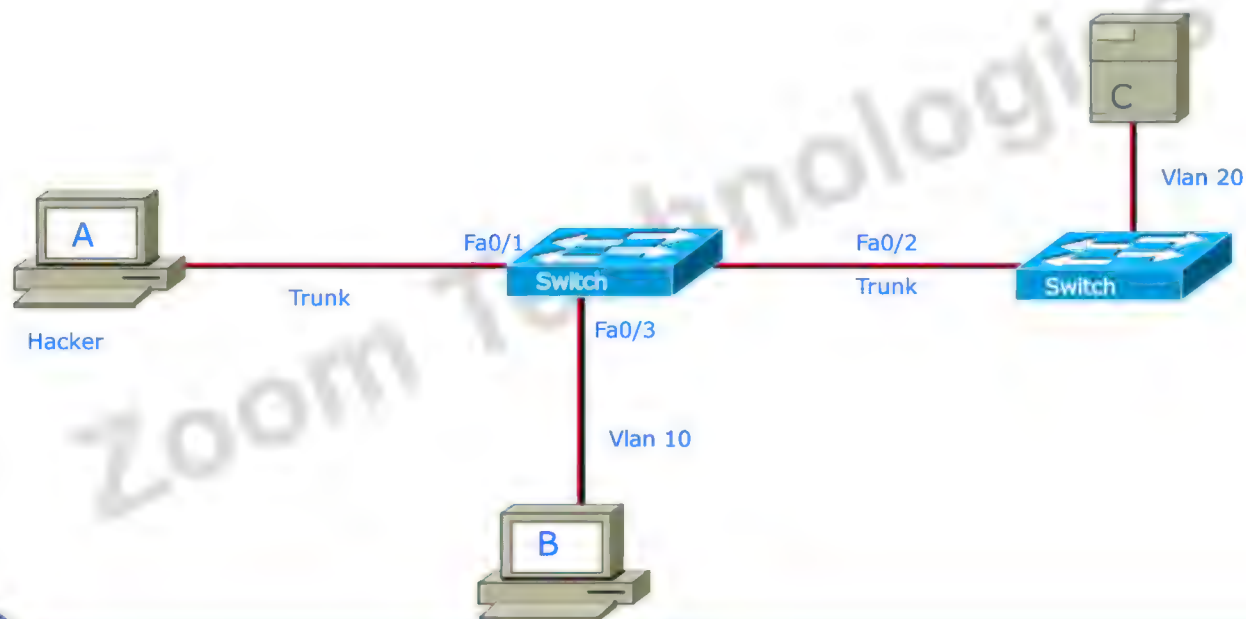


Verification of port security

Switch#show port-security

```
Switch#show port-security
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
              (Count)        (Count)        (Count)
-----
Fa5/1             11             11             0                Shutdown
Fa5/5             15             5              0                Restrict
Fa5/11            5              4              0                Protect
-----
Total Addresses in System: 21
Max Addresses limit in System: 128
```





- Used to filter traffic within one Vlan
- It is configured using access-map
- It is implemented per VLAN
- It can filter the traffic base on MAC
- Extended MAC list is Required



Creating Extended MAC ACCESS list

s(c)#mac access-list extended zoom

s(c-ext-macl)#permit 0000.0000.000a 0000.0000.0000 0000.0000.000b 0000.0000.0000

Creating Access-map

s(c)#vlan access-map V10 10

s(c-access-map)#match mac address zoom

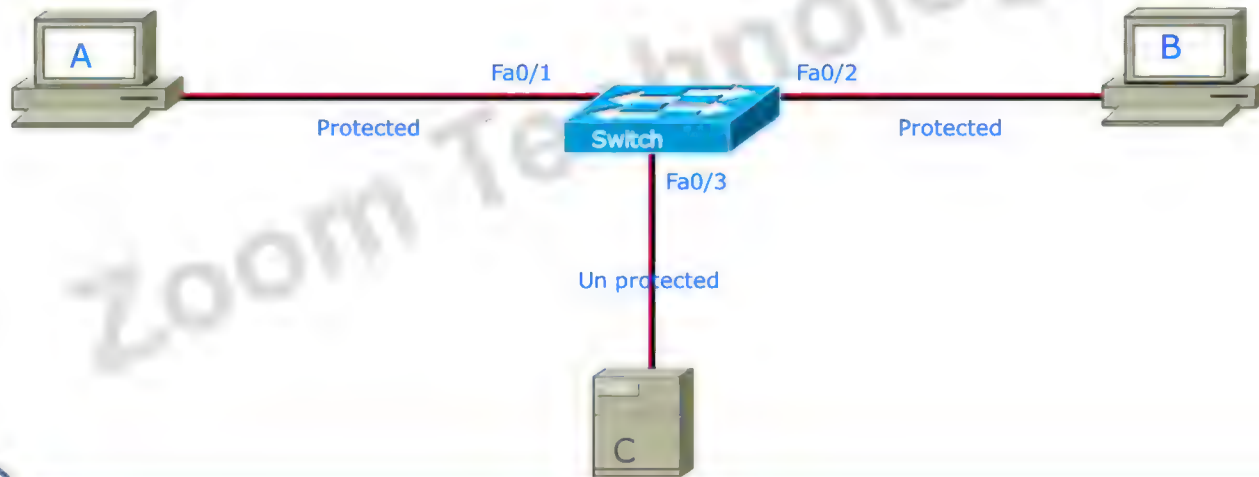
s(c-access-map)#action drop | forward

Implementing

s(c)#vlan filter v10 vlan-list 10



Protected port is a feature on Cisco switches that is used to prevent interfaces are communicating with each other.



- DHCP spoofing is a type of attack in that the attacker listens for DHCP Requests from clients and answers them with fake DHCP Response before the authorized DHCP Response comes to the clients.
- The fake DHCP Response often gives its IP address as the client default gateway -> all the traffic sent from the client will go through the attacker computer, the attacker becomes a "man-in-the-middle".
- The attacker can have some ways to make sure its fake DHCP Response arrives first. In fact, if the attacker is "closer" than the DHCP Server then he doesn't need to do anything. Or he can DoS the DHCP Server so that it can't send the DHCP Response.

"Here you go, I might be first!" (Rogue)

"I can now forward these on to my leader." (Rogue)

"Here you go." (Legitimate)

Legitimate DHCP Server

Rogue DHCP Attacker

Client

"I need an IP address/mask, default gateway, and DNS server."

"Got it, thanks!"

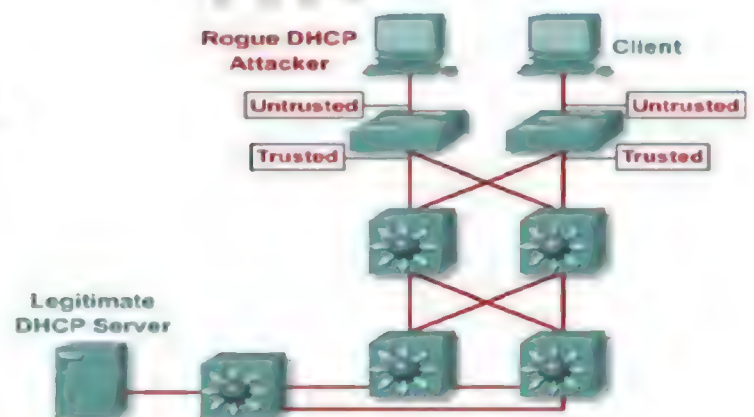
"Already got the info."

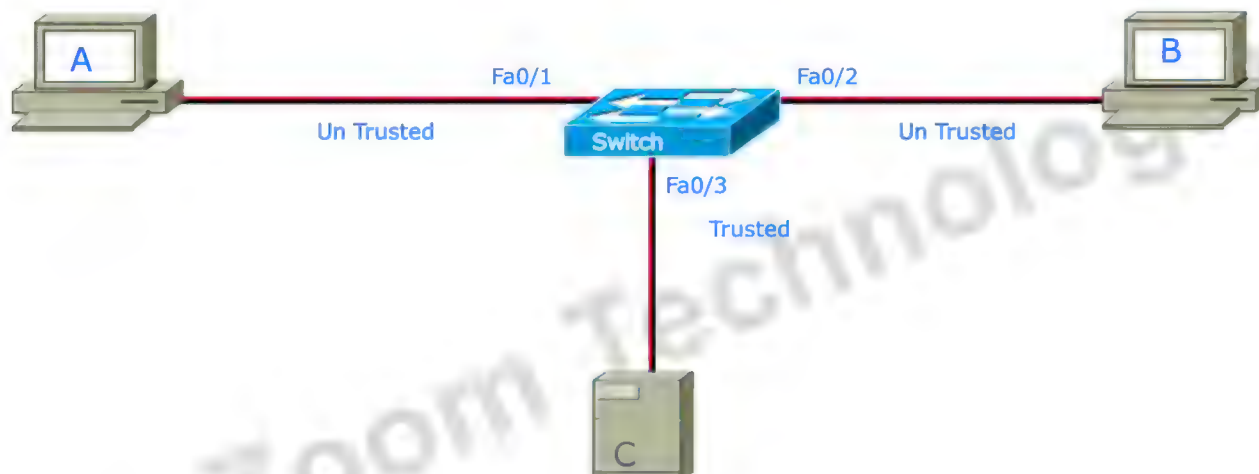
All default gateway frames and DNS requests sent to Rogue.



DHCP Snooping

- Cisco Catalyst feature that determines which switch ports can respond to DHCP requests.
- Trusted ports can source all DHCP messages while untrusted ports can source requests only. Should not send any DHCP server responses, such as DHCPOFFER, DHCPACK, or DHCPNAK
- If a rogue device on an untrusted port attempts to send a DHCP response packet into the network, the port is shut down.





DHCP Snooping Configuration

- Switch(config)#ip dhcp snooping

```
Switch(config)#ip dhcp snooping
```

- Enable DHCP snooping globally

```
Switch(config)#ip dhcp snooping information option
```

- Enable DHCP Option 82 data insertion

```
Switch(config-if)#ip dhcp snooping trust
```

- Configure a trusted interface

```
Switch(config)#ip dhcp snooping vlan number [number]
```

- Enable DHCP snooping on your VLANs

Switch(config)#ip dhcp snooping
(enable dhcp snooping globally)

Switch(config-if)#ip dhcp snooping trust
(configure trusted interface)

Switch(config)#ip dhcp snooping vlan number[number]
(enable dhcp on vlans)



Switch#show ip dhcp snooping

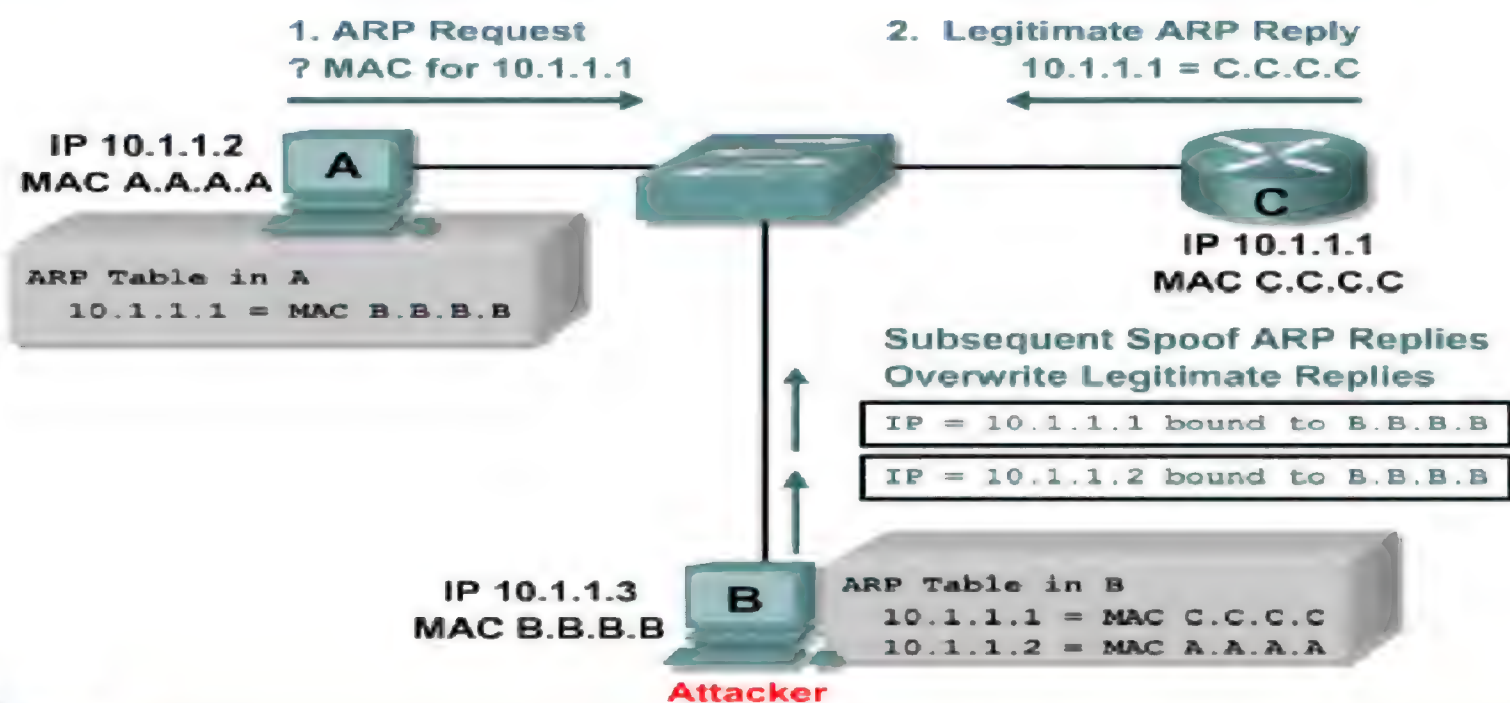
- Verify the DHCP snooping configuration

```
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP Snooping is configured on the following VLANs:
 10 30-40 100 200-220
Insertion of option 82 information is enabled.
Interface           Trusted           Rate limit (pps)
-----
FastEthernet2/1      yes              none
FastEthernet2/2      yes              none
FastEthernet3/1      no               20
Switch#
```



- ARP Spoofing is a type of attack where attacker sends fake arp messages to implement man in the middle attacks.
- Dynamic ARP inspection prevents ARP spoofing by checking all ARP requests and ARP replies.
- DHCP snooping must be configured before enabling DAI.
- Dynamic ARP Inspection uses DHCP snooping binding table to protect against ARP spoofing attacks.
- The switch checks the MAC to IP binding in the ARP reply with the DHCP snooping database.
- Drops invalid ARP replies.

ARP Spoofing



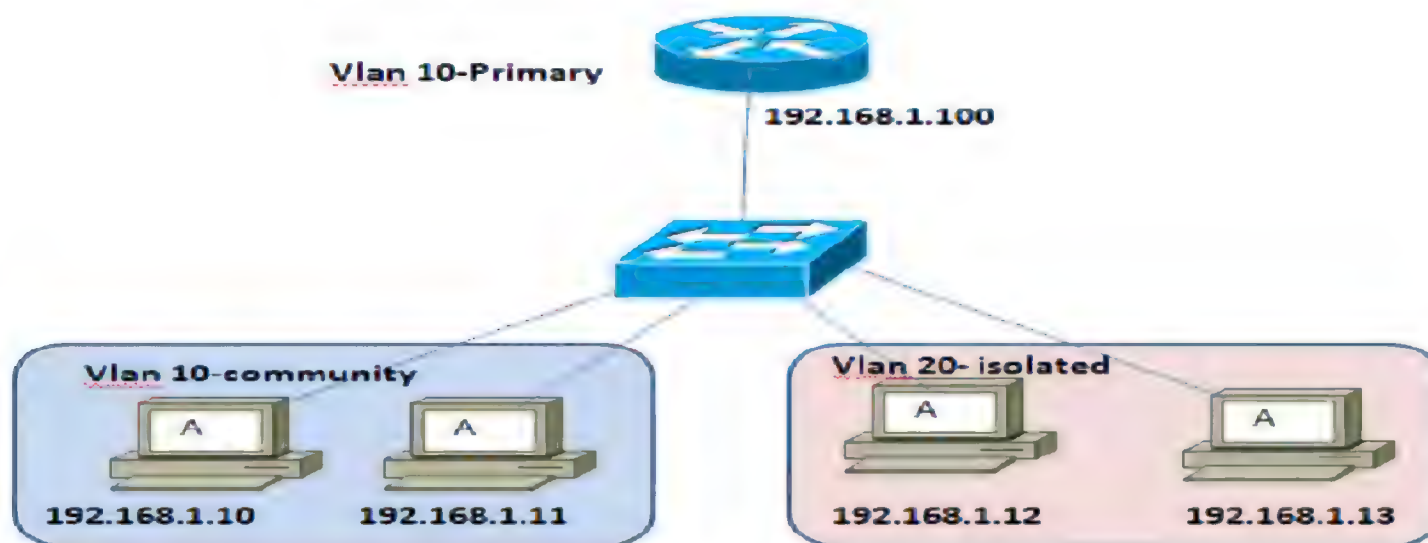
DHCP SDB :

IP Addr	VLAN	MAC	LeaseTime	Port	Checksum
10.1.1.1	22	00e0.fc5a.0e1b	3EBE2881	Gi1/1	e5e1e733
10.1.1.26	22	00e0.2245.3c4c	34ABE45E	Fe3/8	a111f69b
...					



Configure DAI on switch:

Switch(config)#ip arp inspection vlan < vlan-range>



- Private vlan = vlan inside of vlan
- Private-vlans mainly used by service provider networks.
- Private vlan is the combination of primary and secondary vlan.
- Primary vlan's are same as normal vlans

Secondary vlans will work in two modes

- **Community** : Ports belong to this vlan will communicate with each other
- **Isolated** : Ports belong to this vlan will not communicate with each other

Port assigned to Private vlan will work in two modes

- **Host** : belongs to one private vlan
- **Promiscuous** : belongs to multiple private vlan



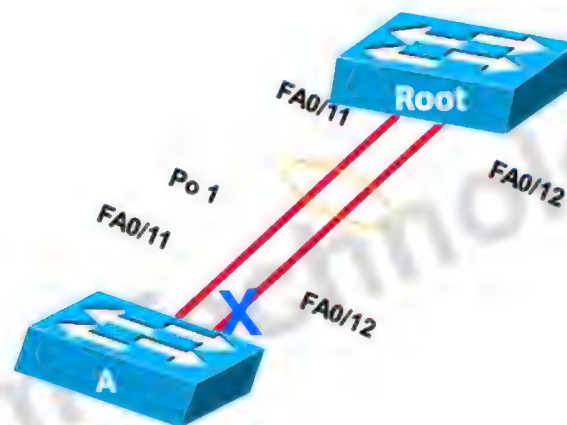
- Storm control is the method to control the traffic on particular interface.
- There are 3 kinds of traffic you can manage on the interface
- **Unicast**
- **Multicast**
- **Broadcast**





Switch Path

ZOOM
TECHNOLOGIES

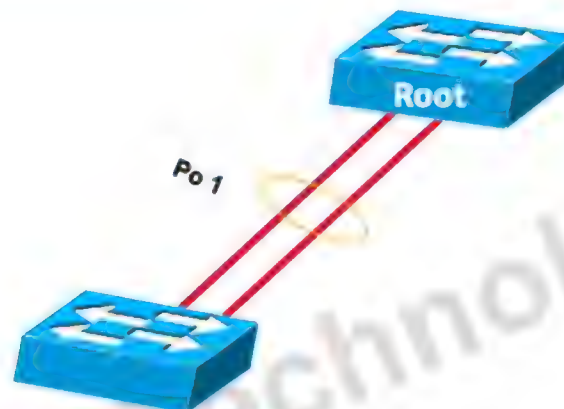


CCIE
CCNP
CCNA

- Logical aggregation of similar links
- Viewed as one logical port
- Switch-level load balancing
- Redundancy
- Can be used between switch to switch, Router, firewall and server

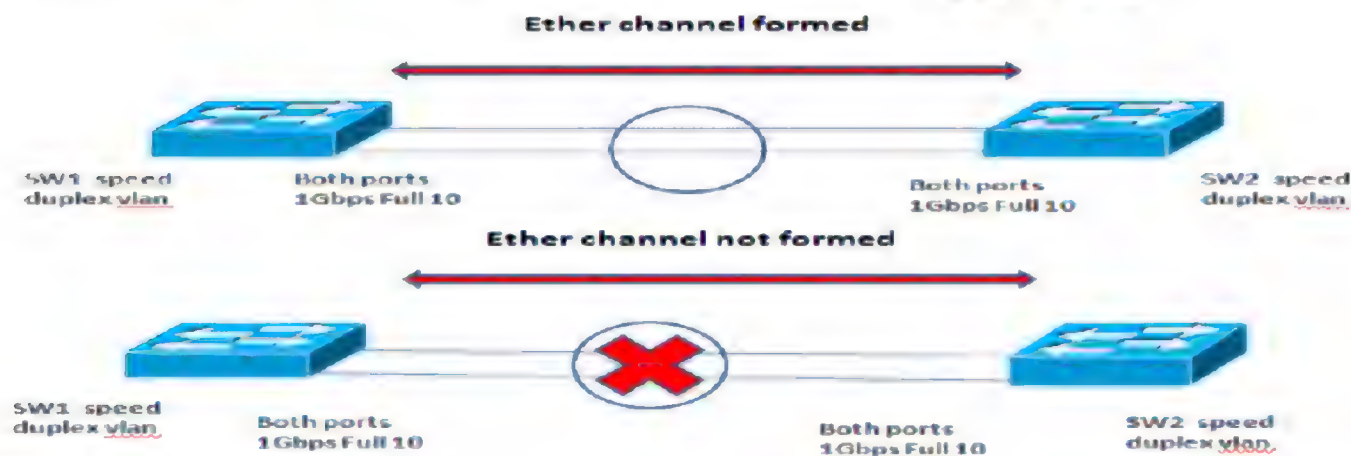
Note:

Only similar physical link with same configuration can be aggregated.
Max 8 similar links can be bundled (depend on Hardware)



- Ether channel configuration can be done in two ways
 - Static (always On mode)
 - Dynamic (using PAgP, LACP)

- EtherChannel must be supported.
- Speed and duplex must match.
- VLAN match – All interfaces are in the same VLAN.
- Range of VLAN – Same range on all interfaces.



- Port Aggregation Protocol (PAgP)
 - Cisco-proprietary protocol
 - PAgP Have two Mode Desirable / Auto
- Link Aggregation Control Protocol (LACP)
 - Defined in IEEE 802.3ad
 - LACP have two mode Active / Passive

```
Switch(config)#interface type <mod/num>
```

```
Switch(config-if)#channel-protocol <pagp/lacp>
```

```
Switch(config-if)#channel-group <no> mode {on | auto |  
desirable | Active | passive }
```

- Configures the interface in a port-channel and specifies the PAgP mode



```
Switch#show running-config interface port-channel num
```

- Displays port-channel information

```
Switch#show running-config interface interface x/y
```

- Displays interface information

```
Switch#show run interface port-channel 1
```

```
Building configuration...
Current configuration:
!
interface Port-channel1
no ip address
no ip directed-broadcast
end
```

```
Switch#show run interface gig 0/9
```

```
Building configuration...
Current configuration:
!
interface GigabitEthernet 0/9
no ip address
channel-group 1 mode desirable
end
```



```
Switch#show etherchannel num port-channel
```

- Displays port-channel information after configuration

```
Switch#show etherchannel 1 port-channel
```

```
Port-channels in the group:
```

```
Port-channel: Po1
```

```
-----
Age of the Port-channel   = 01d:01h:31m:38s
Logical slot/port        = 1/0           Number of ports = 2
GC                        = 0x00020001    HotStandBy port = null
Port state                = Port-channel Ag-Inuse
```

```
Ports in the Port-channel:
```

Index	Load	Port	EC state
0	00	Gi0/9	desirable-sl
0	00	Gi0/10	desirable-sl

```
Time since last port bundled: 00d:20h:04m:38s   Gi0/9
Time since last port Un-bundled: 00d:21h:17m:20s   Gi0/10
```



Ether Channel Load balancing

- Data sent across an Ether Channel is not load-balanced equally among all interfaces.
- Ether Channel utilizes a load-balancing algorithm, which can be based on several forms of criteria, including:



Ether Channel Load balancing



- Source IP Address (src-ip)
- Destination IP Address (dst-ip)
- Both Source and Destination IP (src-dst-ip)
- Source MAC address (src-mac)
- Destination MAC address (dst-mac)
- Both Source and Destination MAC (src-dst-mac)
- Source TCP/UDP port number (src-port)
- Destination TCP/UDP port number (dst-port)
- Both Source and Destination port number (src-dst-port)



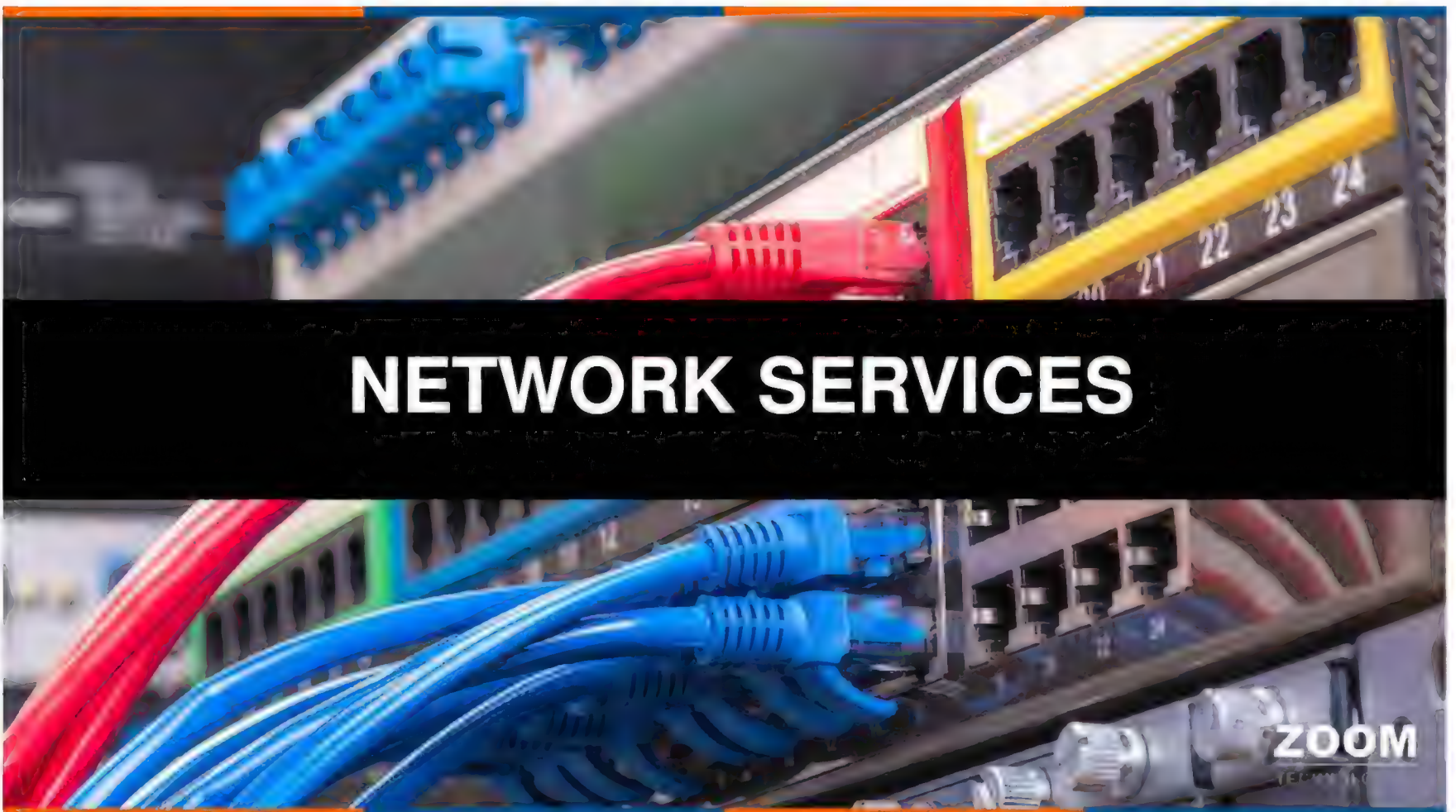
Configuring EtherChannel Load Balancing



```
Switch(config)#port-channel load-balance type
```

- Configures EtherChannel load balancing







Simple Network Management Protocol

ZOOM
TECHNOLOGIES

- SNMP is a protocol used for network management, i.e. to monitor and configure devices on IP networks.
- SNMP works in Application Layer (Layer 7)
- SNMP uses UDP
- SNMP uses port No. 161

Zoom Technologies



- **SNMP MANAGER**
- **SNMP AGENT**

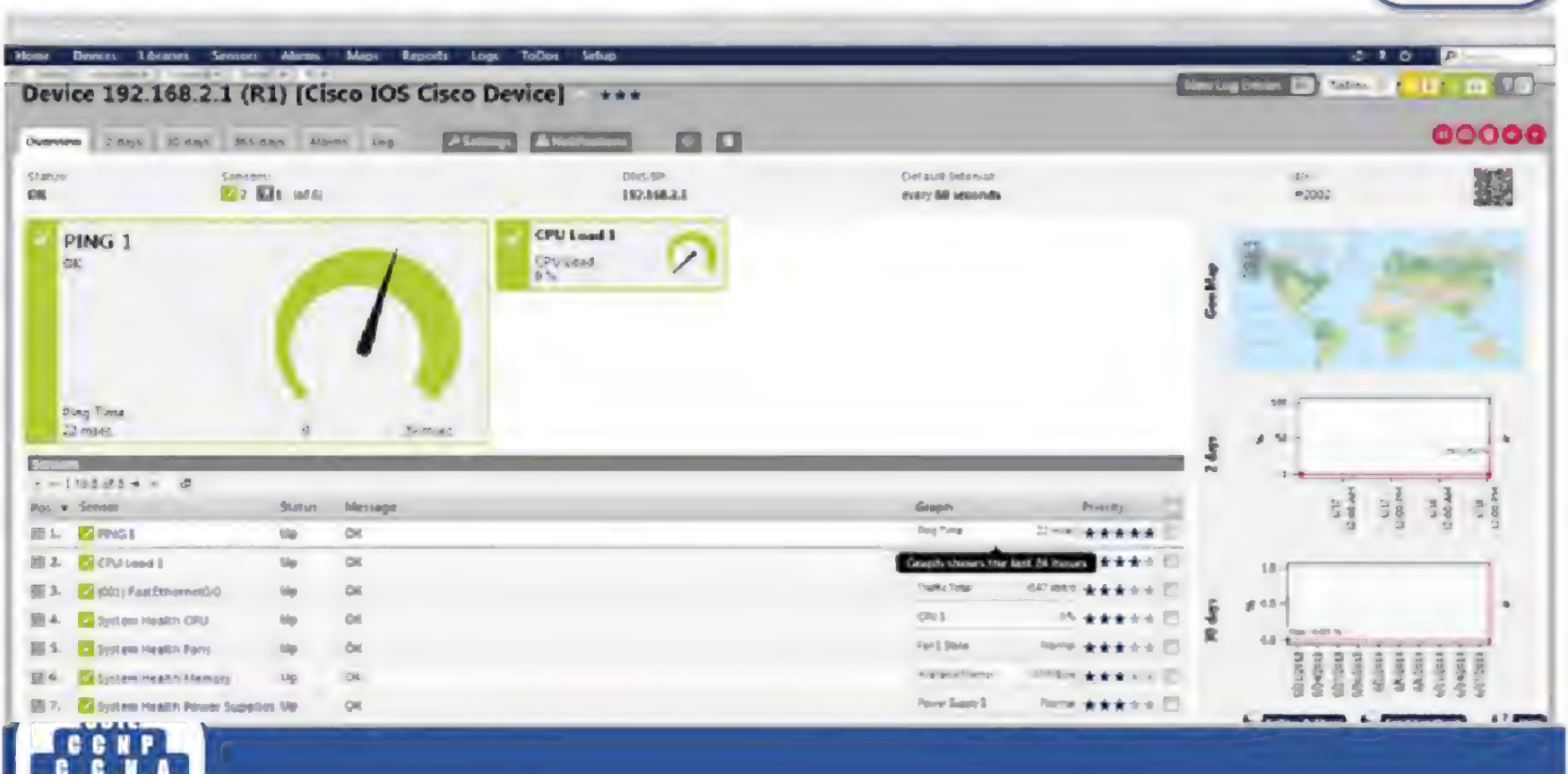
Zoom Technologies

- **Monitor Network Performance**
- **Audit Network Usage**
- **Detect Network Faults**
- **Detect Inappropriate access**
- **Configure remote devices**



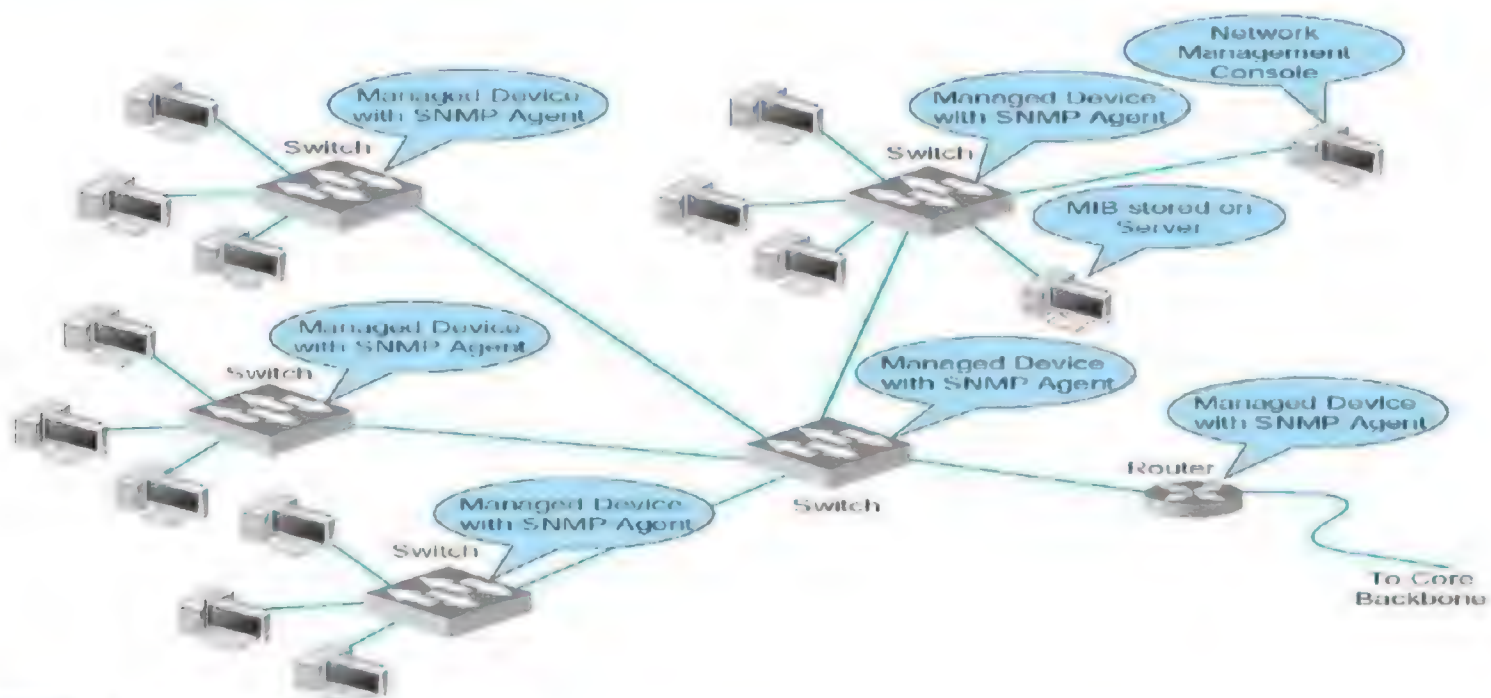
- SNMP Manager is a software that collects information from network devices.
- SNMP Manager is installed on a workstation or PC to manage the network. We call this PC or Workstation as Network Management System.
- EX: PRTG, Cisco Prime , Solar Winds

Zoom Technologies



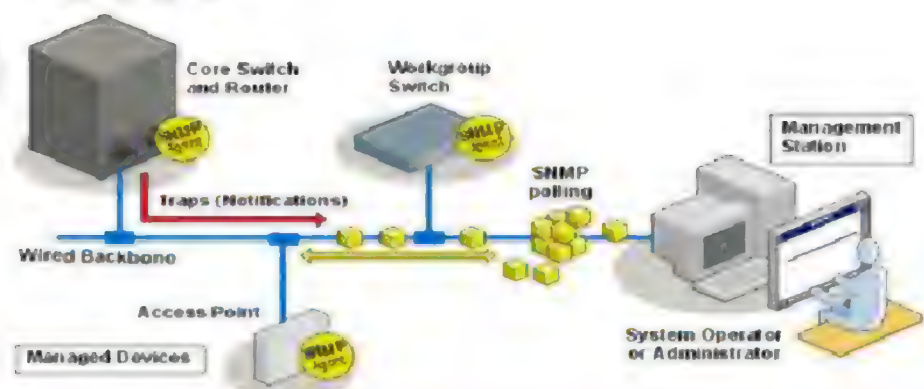
- SNMP Agent is the software that is installed on network managed devices such as Router (or) Switch (or) Server (or) PC.
- Agents collect information and then send it to monitoring station whenever it is asked.
- Agents are usually built into your network hardware and software. They simply need to be enabled.

Zoom Technologies



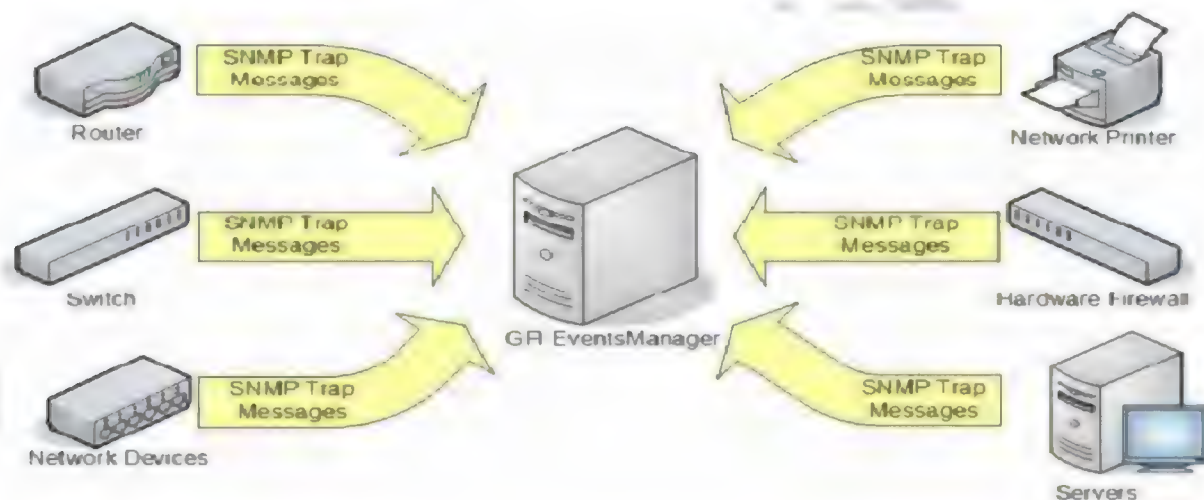
Polling

- In Polling method, SNMP Manager continuously asks a network device to report the statistics of device.
- Example: Interface Status of Router.
- Request is sent from SNMP Manager to Agent.



TRAP

- Trap is where device reports an event to NMS, for example whenever High CPU utilization or High Memory Utilization or Link Down is detected.



- **Read – Only Mode:**
 - used to retrieve information from network devices.
- **Read – Write Mode**
 - Used to retrieve the information from network devices as well as to configure the devices.

- **Management Information Base (MIB)** contains collection of information which is organized hierarchically.
- **Management Information Base contains-**
 - Object name
 - Object Identifier
 - Read/Only or Read/Write Type



SNMP Versions

- SNMP V1
- SNMP V2
- SNMP V3

Zoom Technologies

- It is the initial version of SNMP Protocol.
- Data is sent in the clear text format.
- It should be used in private networks only.
- They use the community string to authenticate the peers.
- Uses Get Request to retrieve the information about particular object.

- SNMP Version 2 is the enhanced version of SNMP.
- Improved Error Handling and Error Reporting
- Get Bulk Request command is used to retrieve the information .
- It also uses community string to authenticate the peers.

- Provides secure access using authentication and encryption.
- Consumes more CPU memory compared to other versions.
- It defines 3 Security levels.

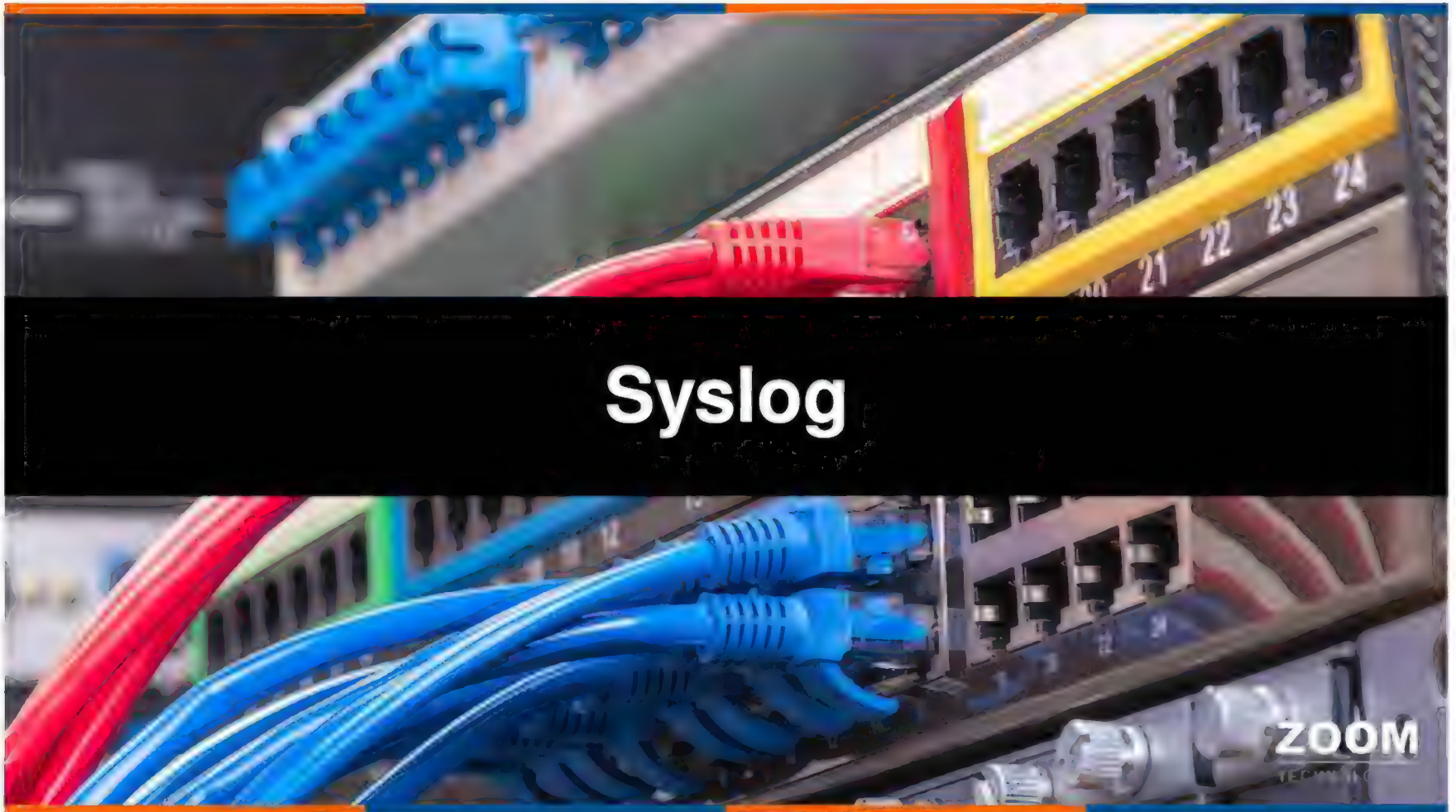


SNMP configuration

Requirement:

- Configure SNMP on your router or switch
- Router(config)#snmp-server enable traps
- Router (config)#snmp-server host 192.168.0.50 version 2c public
- Router(config)#snmp-server location Hyderabad
- Router(config)#snmp-server contact zoomgroups





What is Syslog

ZOOM
TECHNOLOGIES

- Syslog is a standard for message logging.
- Syslog is a network management protocol which allows network devices to report error and notification messages either locally (or) to a remote syslog server.
- Syslog messages are sent in plain text using UDP port No. 514.

Zoom Technologies



- **Syslog Server**
 - A host that accepts and processes log messages from 1 or more syslog clients.
- **Syslog Client**
 - A host that generates log messages and forwards them to a syslog server.
 - Ex: Router, switch, firewall, modem

Facility Mnemonic

%SYS-5-CONFIG_I: Configured from console by console
Severity

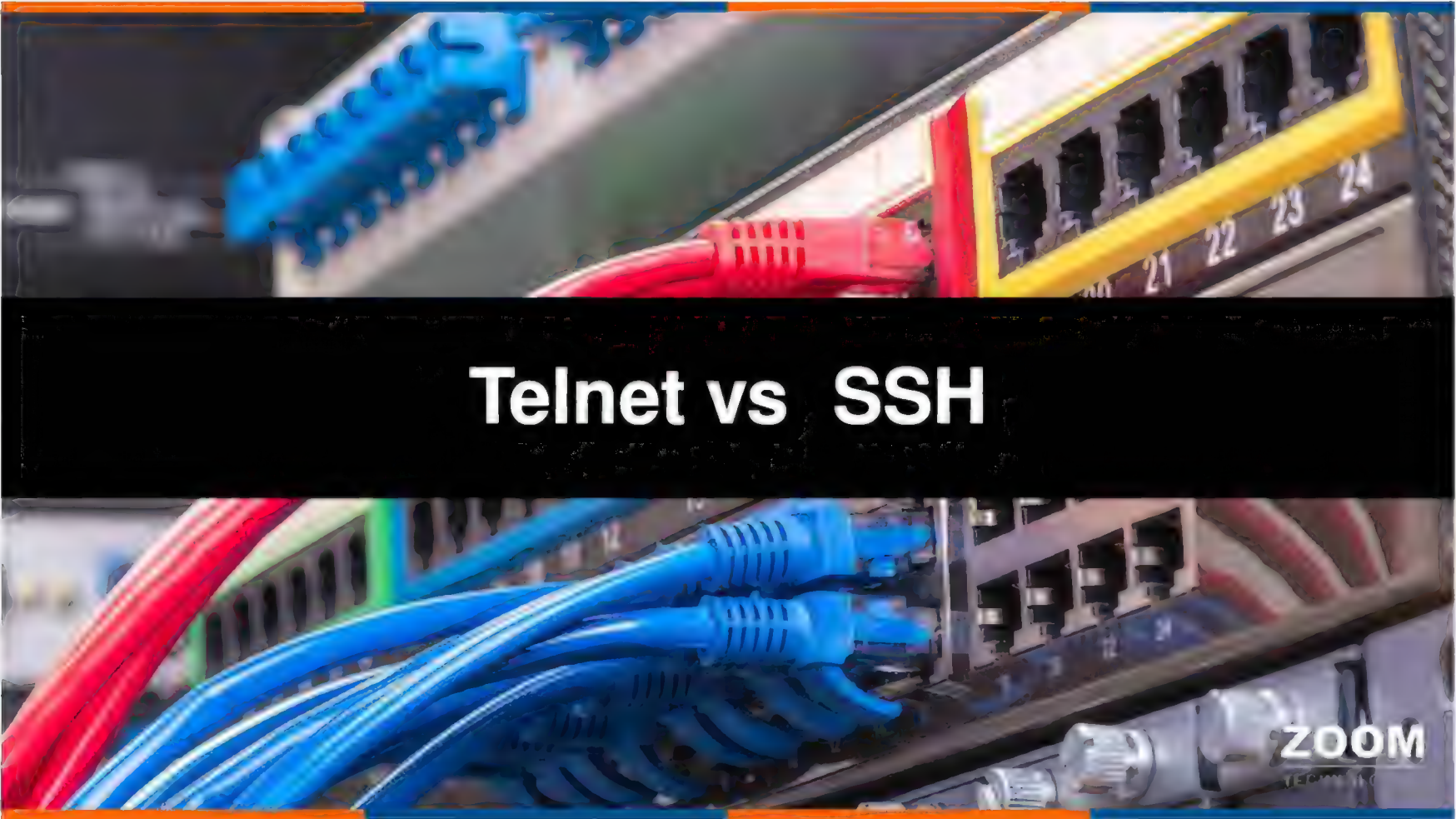


Configure syslog

Requirement:

- *Configure syslog server to store the messages in a server.*
- *R1(config)# logging on*
- *R1(config)#logging 192.168.0.50*
- *R1(config)#logging trap i4*
- *Verification:*
- *R1#show logging*





Telnet vs SSH

ZOOM
TECHNOLOGIES

Telnet	SSH
Port No. 23	Port No. 22
Uses TCP	Uses TCP
Not Secured	Secured
Works in Application Layer (Layer 7)	Works in Application Layer (Layer 7)

Telnet

- Telnet is a protocol which allows you to access any device remotely.
- It sends the data in Clear-Text format.

SSH

- SSH is a protocol which allows you to access any remote device securely
- It sends the data in Encrypted format.

SSH configuration

- **Requirement:**
- **Configure SSH on SW1.**
- **SW1(config)#hostname ssh**
- **SW1(config)#ip domain-name zoom.com**
- **SW1(config)#crypto key generate rsa**
- **SW1(config)# line vty 0 4**
- **SW1(config-line)# transport input ssh**
- **SW1(config-line)#login local**
- **SW1(config-line)#password zoom**
- **SW1(config-line)#exit**
- **Verification:**
- **SW1#show ip ssh**



NETWORK TIME PROTOCOL

NTP

ZOOM
TECHNOLOGIES

- Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) is the global standard for time representation.
- Most of the network enabled devices have two clock sources
 - Hardware clock
 - Software clock

Zoom Technologies



- NTP provides accurate timing services to each and every network enabled device.
- It provides automatic synchronization of device clock with one or more time servers which provide accurate time.
- NTP uses UDP port number 123 .

Zoom Technologies

- NTP servers are described in terms of stratum
- (hierarchical levels).
- Stratum defines the accuracy of the clock. The most accurate clock is referred as reference clock or stratum 0 clock.
- Each NTP server assigned a stratum one higher than the upstream device with which is synchronized.

Zoom Technologies

- NTP can be disabled on a particular interface
 - Router(config-if)# ntp disable
- Configure NTP in Cisco Device-
 - R(config)# ntp source <interface>
 - R(config)# ntp authenticate
 - R(config)# ntp authentication-key <number> md5 <key>
 - R(config)# ntp trusted-key <key-number>
 - R(config)# ntp server <ip-address> key <key-id>



- IP SLA is a technology from Cisco that actively monitors traffic to measure the performance of the network.
- Performance of the network can be measured by using following parameters
 - Jitter
 - Latency
 - Packet Loss

- Configure SLA on Router
- R(config)# ip route 0.0.0.0 0.0.0.0 s0/0 Track1
- R(config)# ip route 0.0.0.0 0.0.0.0 s0/1 20
- R(config)# track 1 rtr 1
- R(config)# ip sla 1
- R(config)# icmp-echo 30.1.0.1 <Destination IP>
- R(config)# frequency 5
- R(config)# exit
- R(config)# ip sla schedule 1 start-time now life forever
- R(config)# end
- R# Show IP SLA Statistic

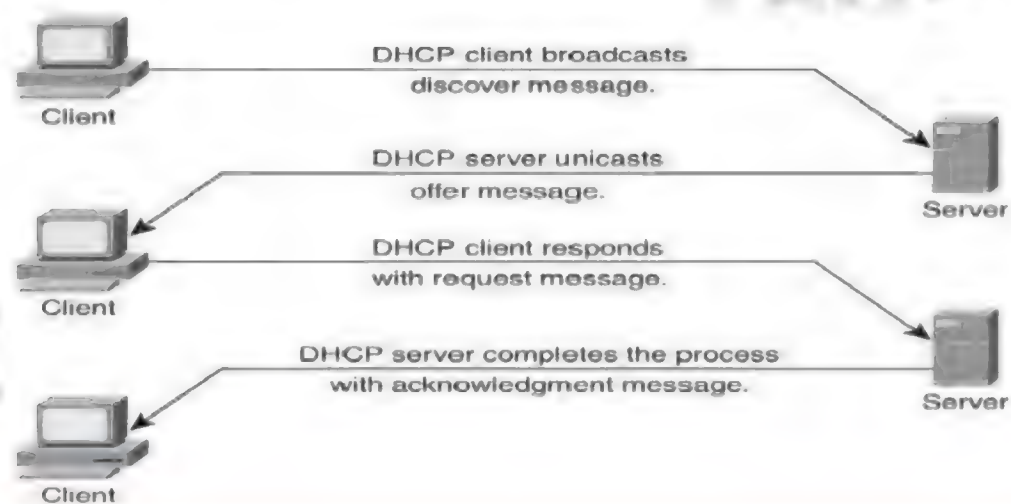
DHCP V4

ZOOM

DHCPV4

ZOOM
TECHNOLOGIES

- DHCP is a dynamic way of assigning network configuration parameters to clients.
- DHCP uses port number 67 and 68.
- DHCP uses DORA process.
- DHCP uses broadcast packets.



CCIE
CCNP
CCNA

- Requirement:
- Configure DHCP server as R1 router.
- **Assign IP address on Lan interface of the R1 router.**
- R1(conf)# interface fastethernet 0/0
- R1(conf-if)# ip address 192.168.5.1 255.255.255.0
- R1(conf-if)# no shutdown
- R1(config)#ip dhcp pool zoom
- R1(dhcp-config)#network 192.168.5.0 255.255.255.0
- R1(dhcp-config)#default-router 192.168.5.1
- R1(dhcp-config)#dns-server 192.168.5.1
- R1(dhcp-config)#end



- R1(config)# ip dhcp excluded-address 192.168.5.1
- R1(config)#ip dhcp pool zoom
- R1(dhcp-config)#lease 1
- Verification:
- R1#show ip dhcp binding



DHCP RELAY AGENT

ZOOM

DHCP Relay Agent

ZOOM
TECHNOLOGIES

- DHCP Relay Agent forwards DHCP messages between DHCP clients and DHCP Servers which reside on different IP network.
- By default router will not forward broadcasts, DHCP relay agent will convert broadcast into unicast packets.



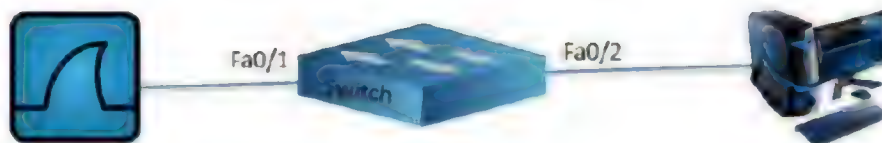
Router(config-if)# ip helper-address <DHCP server IP address>

Zoom Technologies

SPAN and RSPAN

- Switched Port Analyzer (SPAN) is also called Port Monitoring; used for Network Analysis.
- SPAN allows you to select one or more ports for analysis .
- SPAN is used to monitor devices on only one switch.
- Remote SPAN is used to monitor devices on more than one switch .

- Switch(config)#monitor session 1 source interface fa0/2
- Switch(config)#monitor session 1 destination interface fa0/1



```
SW1(config)#vlan 100
```

```
SW1(config-vlan)#remote-span
```

```
SW2(config)#vlan 100
```

```
SW2(config-vlan)#remote-span
```

```
SW1(config)#monitor session 1 source interface fastEthernet 0/1
```

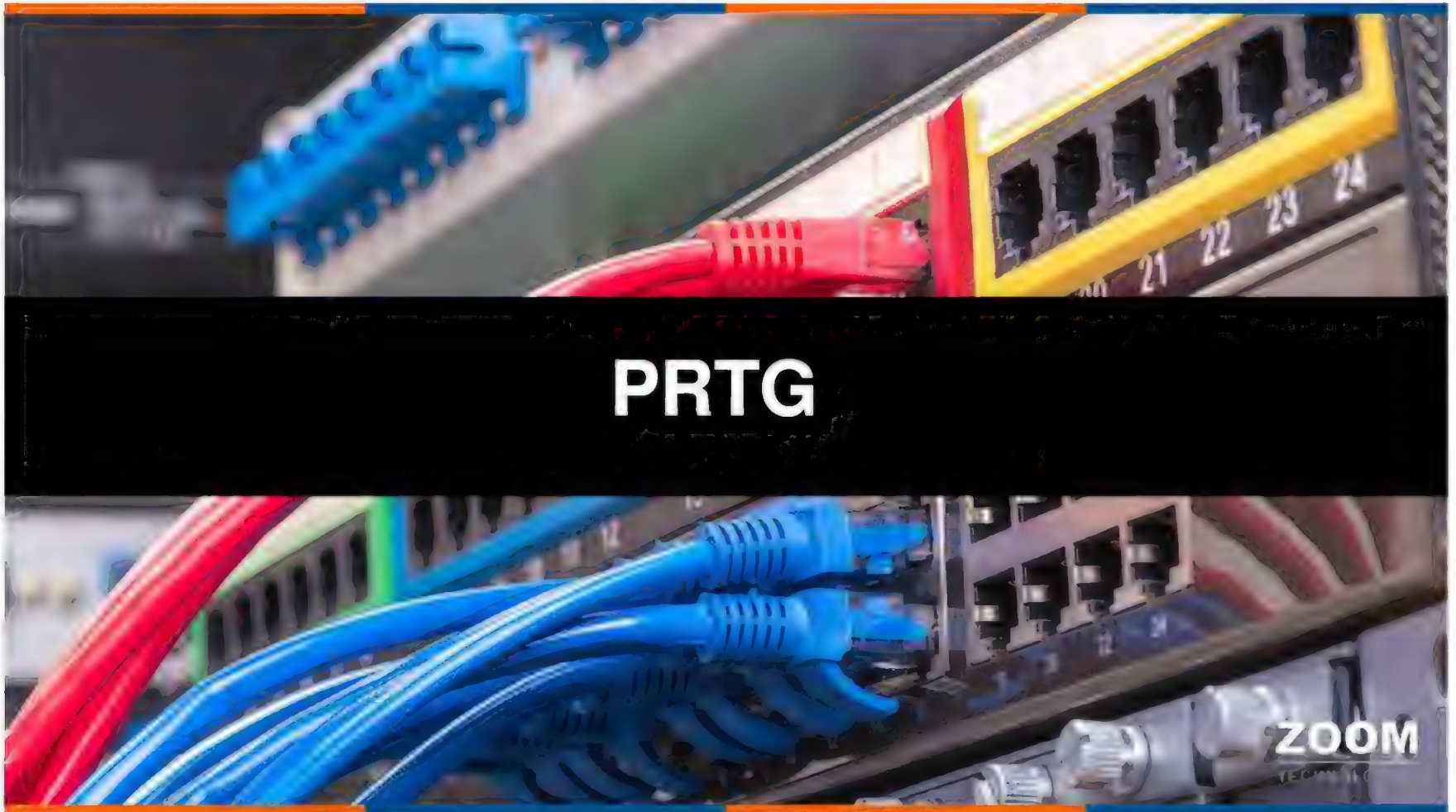
```
SW1(config)#monitor session 1 destination remote vlan 100
```

```
SW2(config)#monitor session 1 source remote vlan 100
```

```
SW2(config)#monitor session 1 destination interface fastEthernet 0/2
```



NETWORK MONITORING TOOL



Agenda

ZOOM
TECHNOLOGIES

- What is Network Monitoring
- Why Monitor Your Network..?
- Where it use
- How it works
- Functions
- About PRTG.
- Some practical things

Zoom Technologies



520

What is Network Monitoring?



- Network Monitoring means continuously monitor a networks **performance**.
- Bandwidth utilization,
- Packet loss,
- Latency(Delay)
- availability and uptime

Why Need To Monitor Network.?

- Optimize network reliability
- Visualize network topology
- Stay in touch with your network
- Understand capacity utilization
- Troubleshoot device and traffic issues
- Save time in network administration
- Track trends
- Improve the bottom line

- Administrators need to know what's happening on their networks at all times
- Track Network performance
- Diagnose problems quickly.
- Keep Record of historical information
- Intelligent notifications (via SMS and mail)
- Save Time & Money....

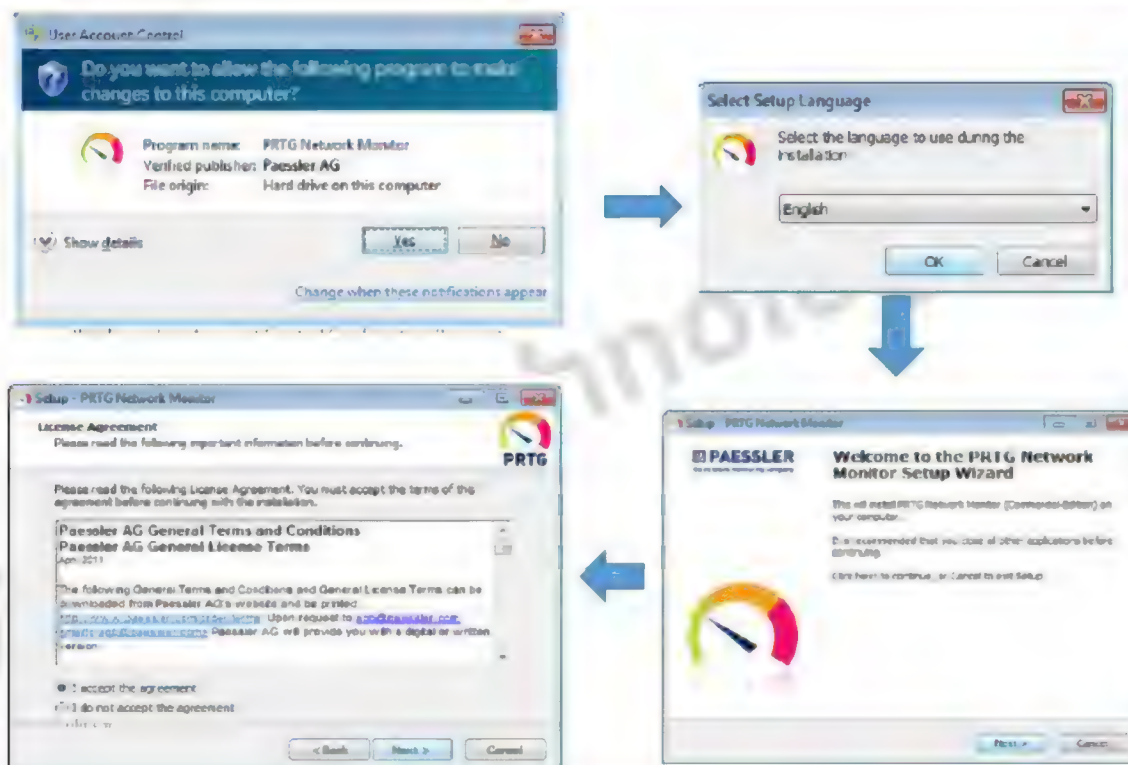


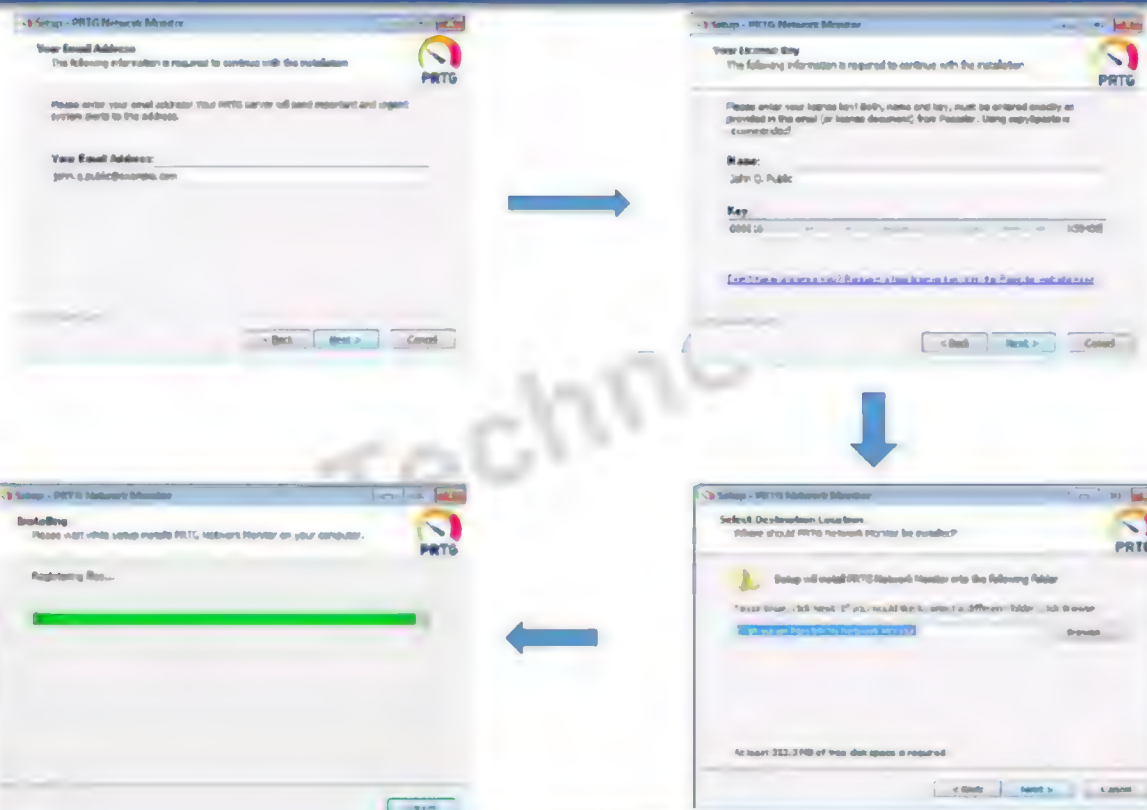
- There are so many network monitoring tools available on global platform.
- Some of them are free and some are paid.
- Free tools have some limitations, It can't give us deep performance information about network.



PRTG is network monitoring software from Paessler AG. PRTG runs on Windows and monitors network availability and network usage using **SNMP, Packet Sniffing, WMI, IP SLAs and Netflow** and various other protocols.

Installation.....





PRTG Network Monitor



PRTG
Network Monitor

Login Name

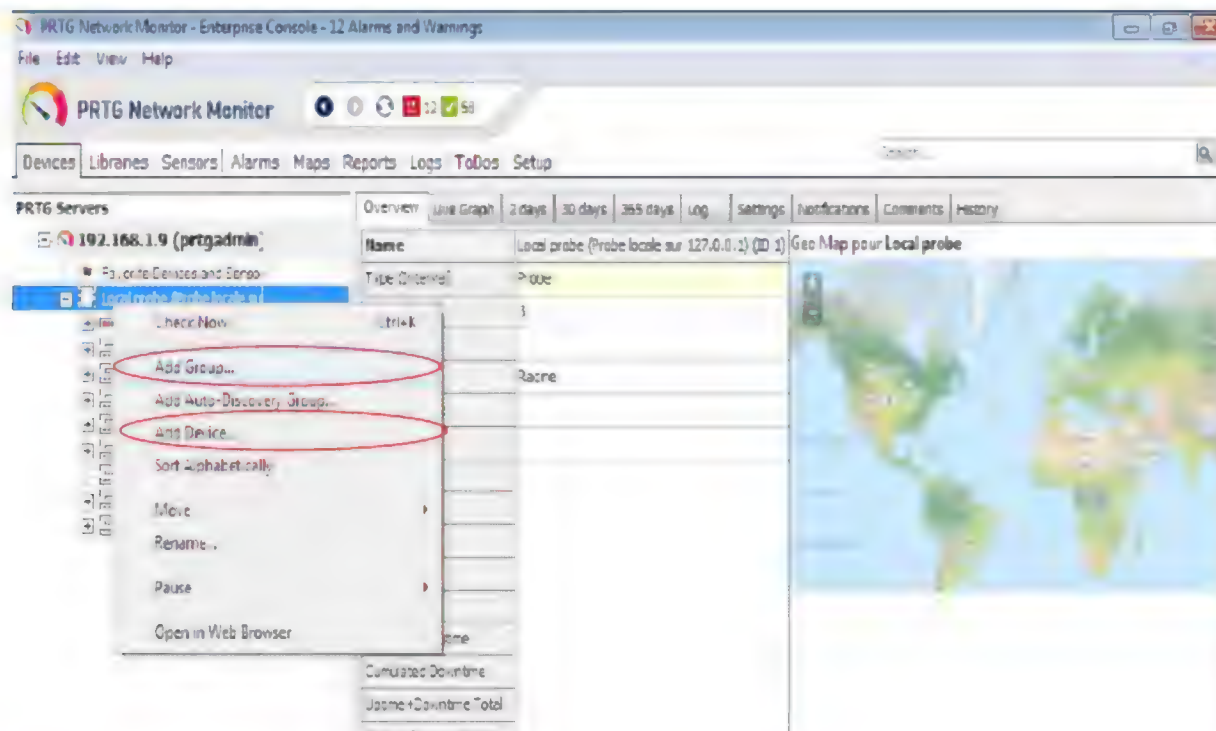
Password

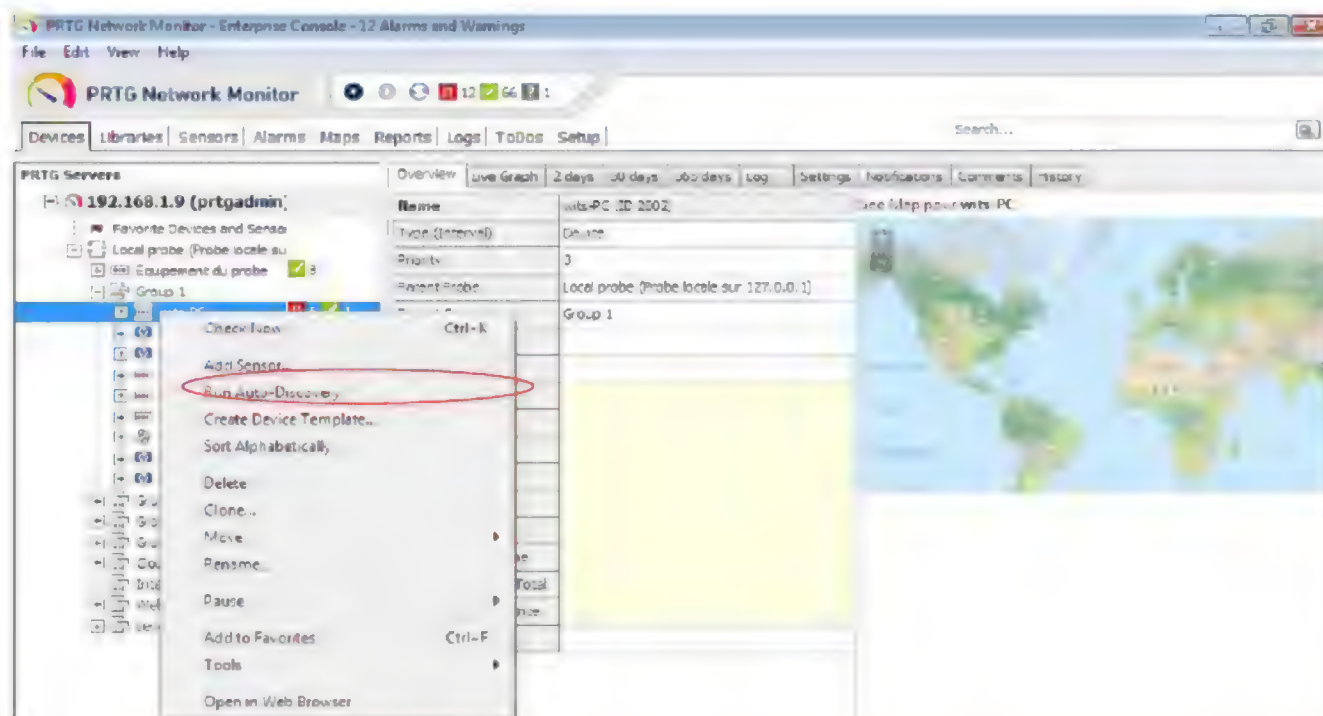
- ☒ AJAX WebGUI (All features, optimized for desktop access)
- ☐ Mobile WebGUI (Limited functionality, optimized for mobile access)
- ☐ Enterprise Console & Mobile Apps (for Windows, iOS, Android)

Login

Default Login

[Forgot password? Need Help?](#)





Why Network Monitoring ?





Saves Time



Saves Money



Offers Security

- PRTG Network Monitor consists of different parts which can be divided into three main categories:
 - **System parts**
 - [Core Server](#)
 - [Probe\(s\)](#)
 - **Control interfaces**
 - [Ajax Web Interface](#)
 - [Enterprise Console](#)
 - [Mobile Web GUI](#)
 - [Smart Phone Apps](#)

- **Basic administration interfaces**
- [PRTG Server Administrator](#)
- [PRTG Probe Administrator](#)

Zoom Technologies



- What is Wireshark
- Where it use
- How it works
- Some practical things



- Network analysis is the process of capturing network traffic and inspecting it closely to determine what is happening on the network.

What is Wireshark.....?



- **Wireshark is a network packet analyzer. A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible.**
- **Previously the packet analyzing was very difficult and it required expensive hardware.**
- **Wireshark is one of the best open source packet analyzer available.**
- **A packet analyzer is also known as a sniffer, network analyzer or protocol analyzer.**



Who and where is tool is use...?



- **Network administrators use it to troubleshoot network problems**
- **Network security engineers use it to examine security problems**
- **Developers use it to debug protocol implementations**
- **People use it to learn network protocol internals**
- **Beside these examples Wireshark can be helpful in many other situations too.**



Shark on Water



Shark on wire



How it works?

ZOOM
TECHNOLOGIES

For Windows

- download
(<http://www.wireshark.org/download.html>)
- install
- use

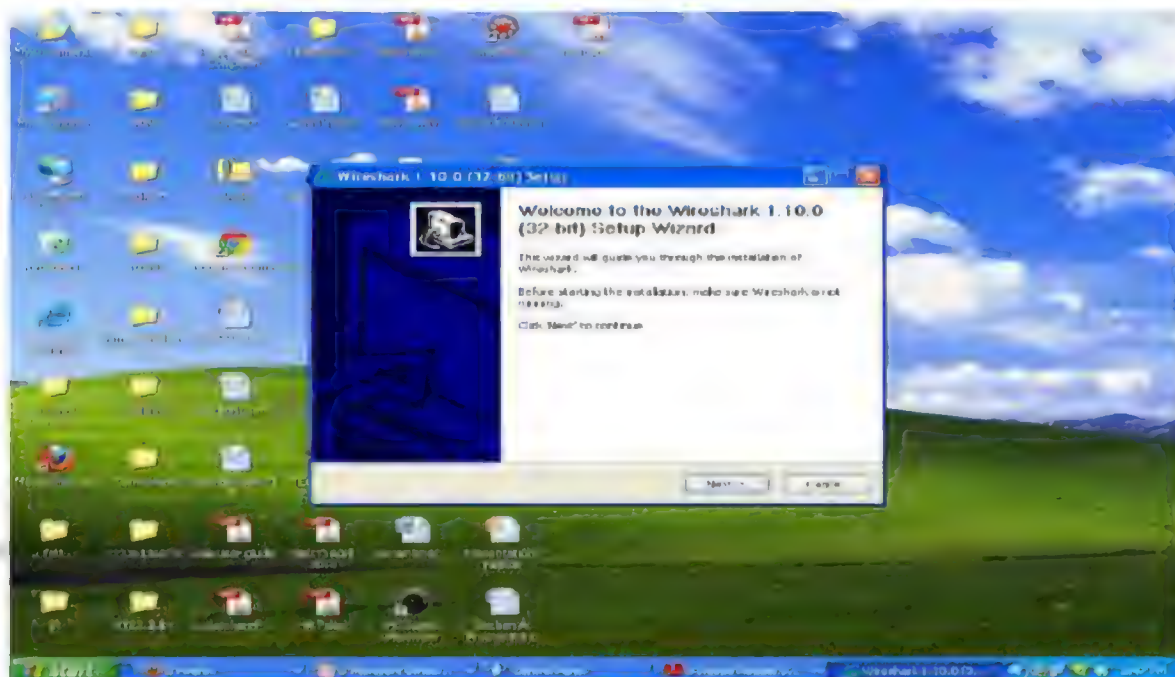


WIRESHARK

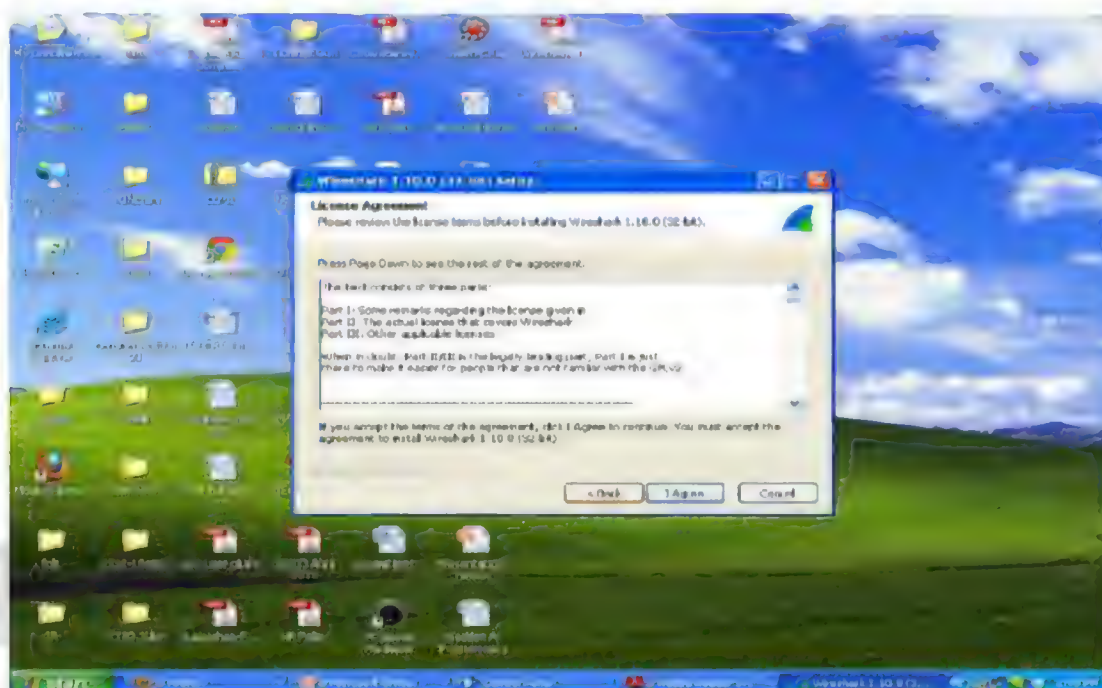
Installation Process

ZOOM
TECHNOLOGIES

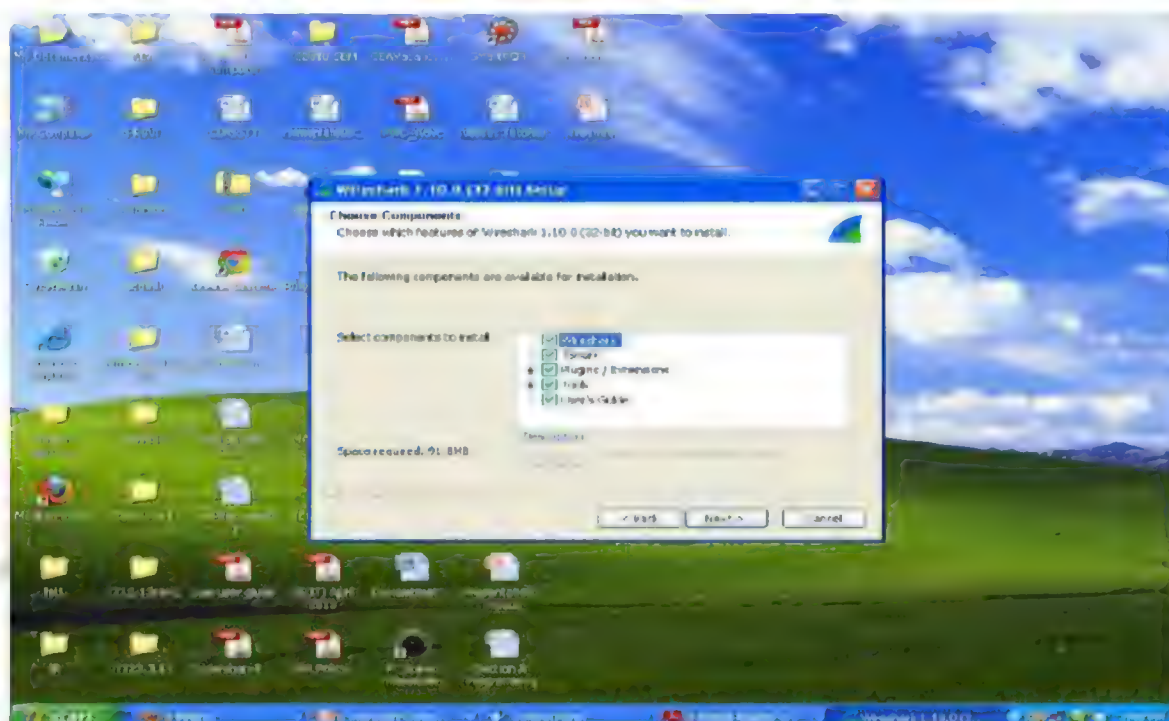
STEP : 1



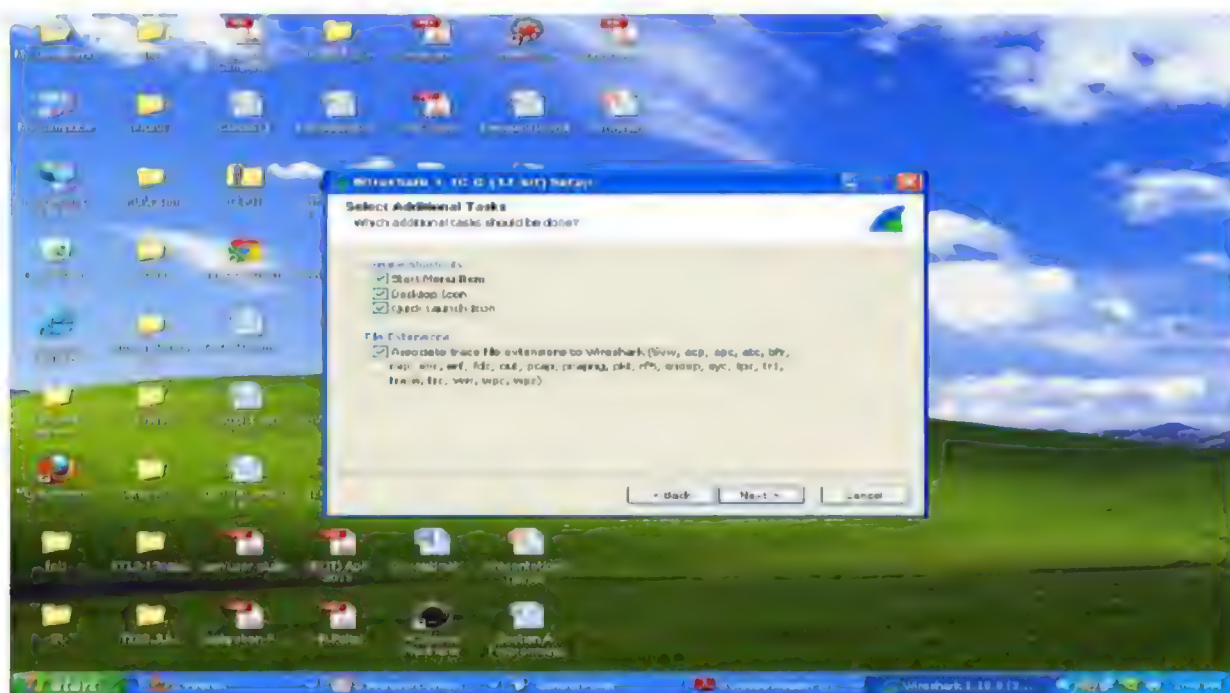
STEP 2:



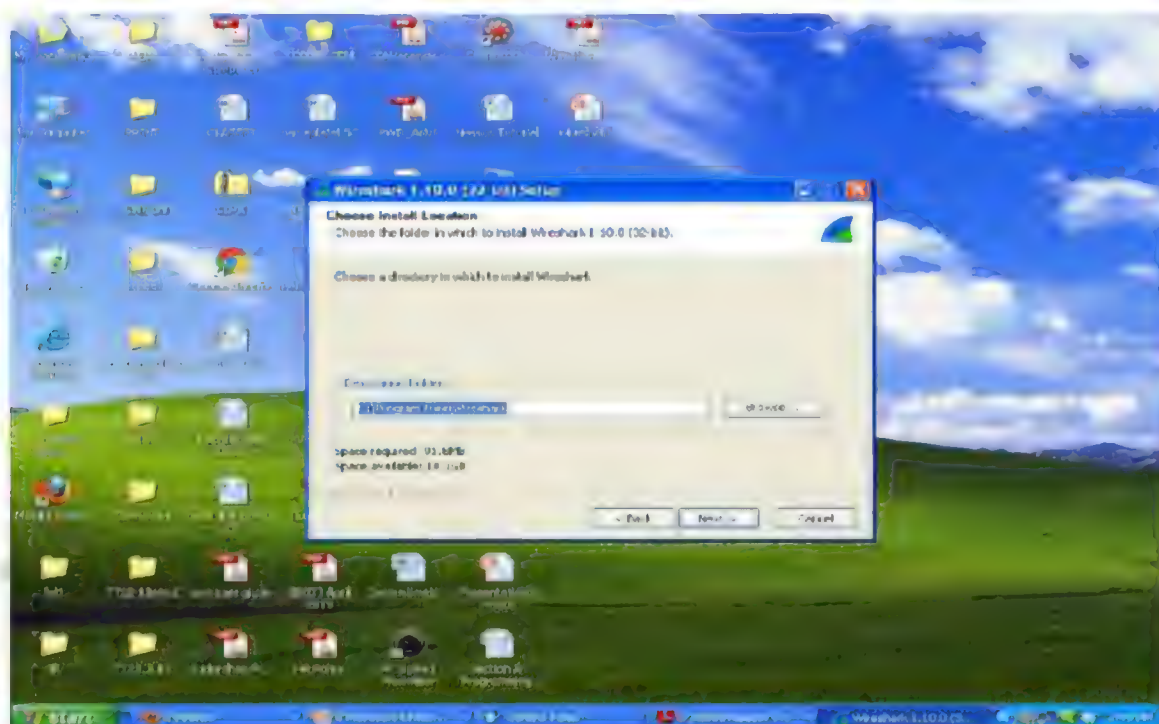
STEP 3:

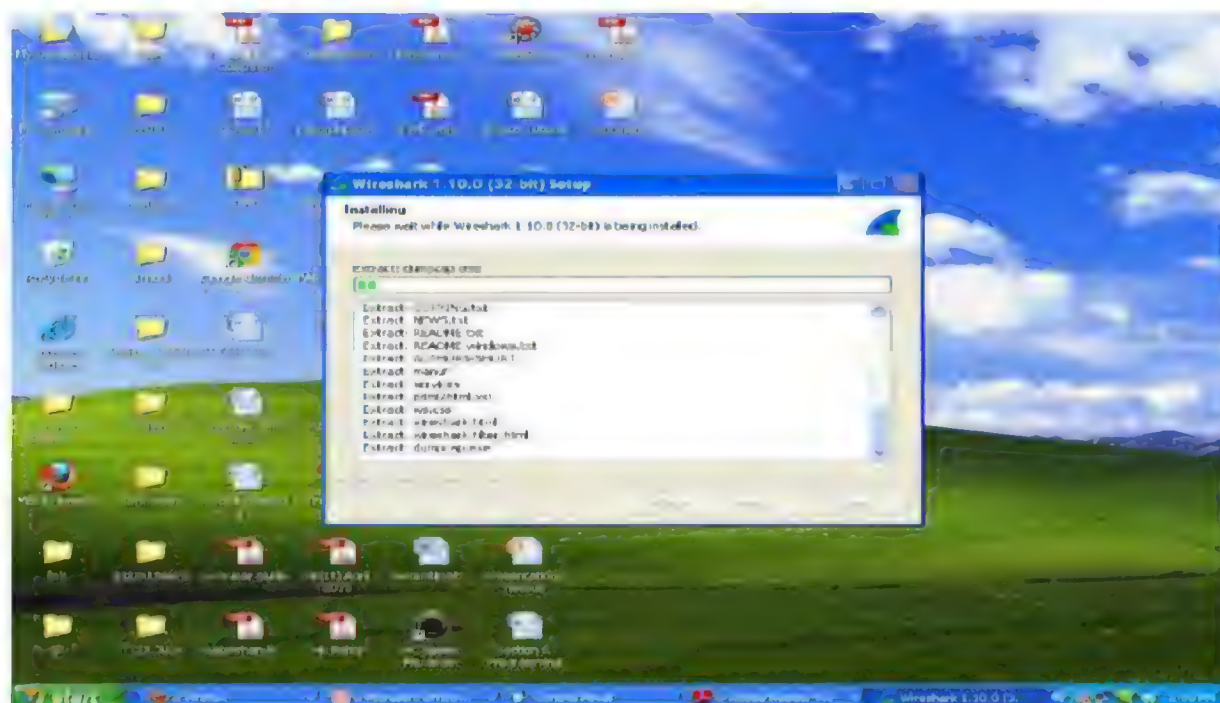
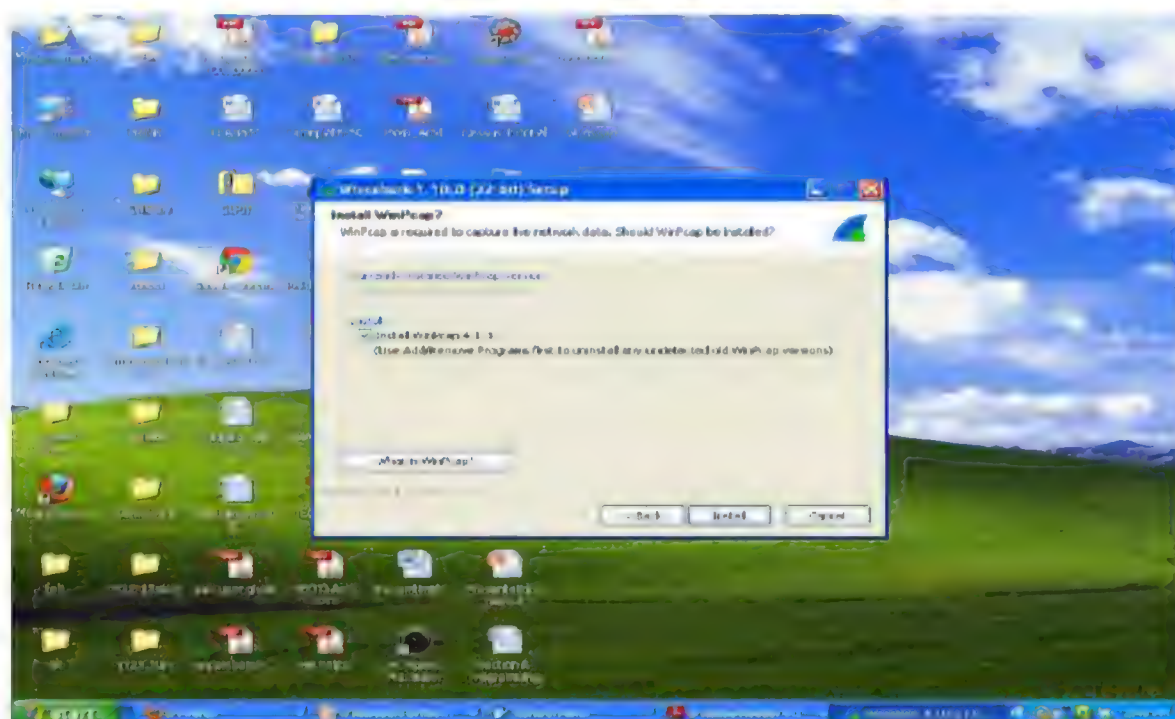


STEP : 4

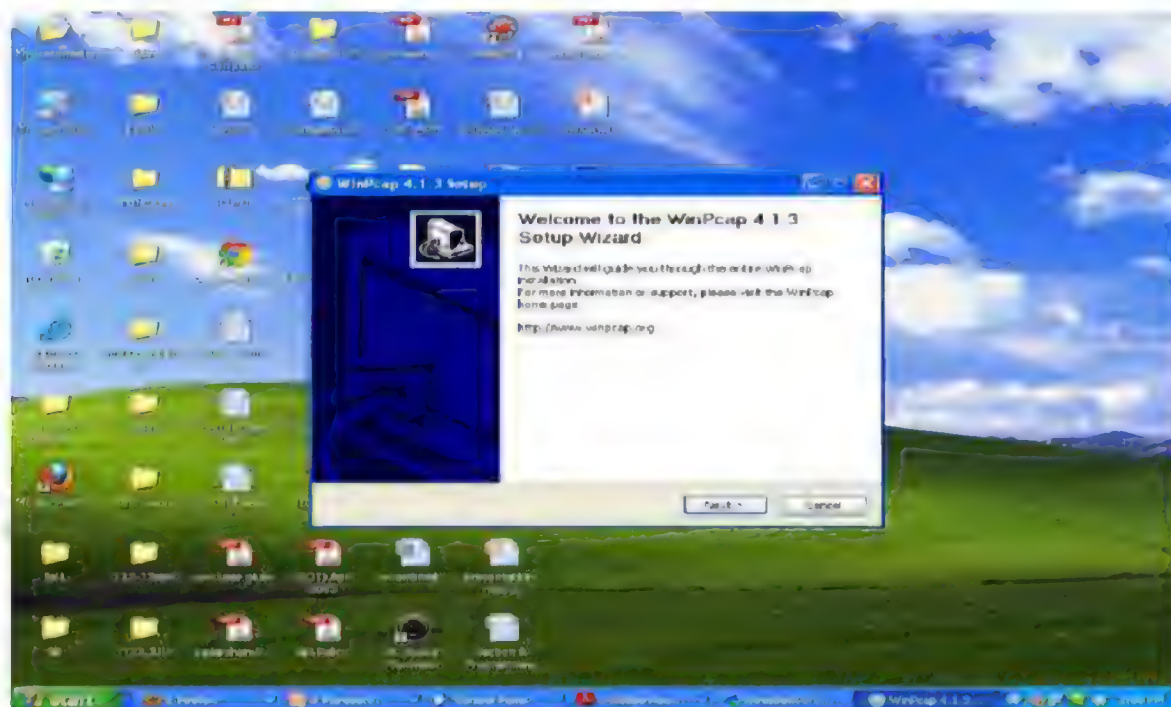


STEP : 5

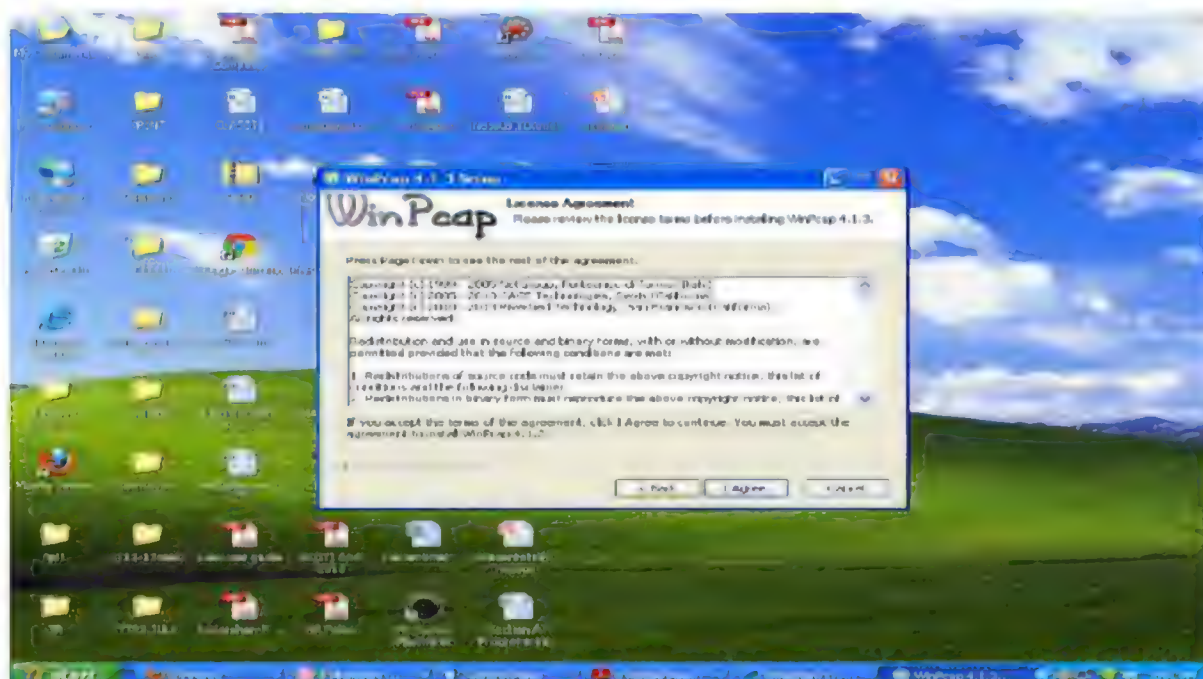


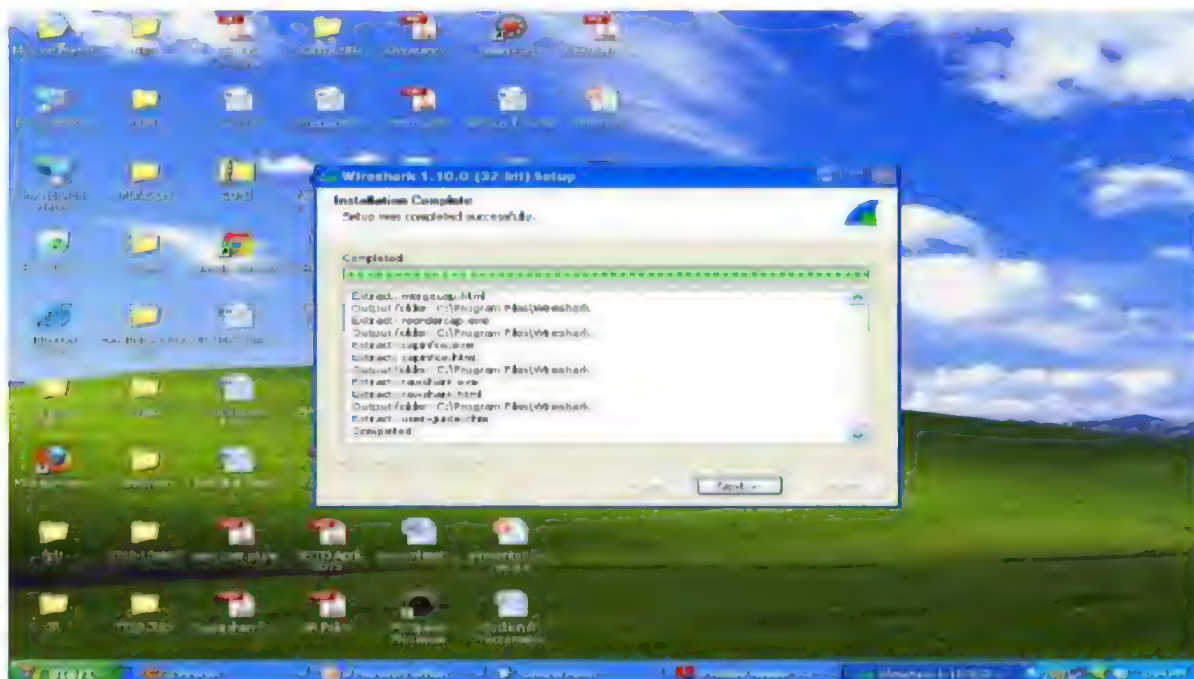


STEP : 8

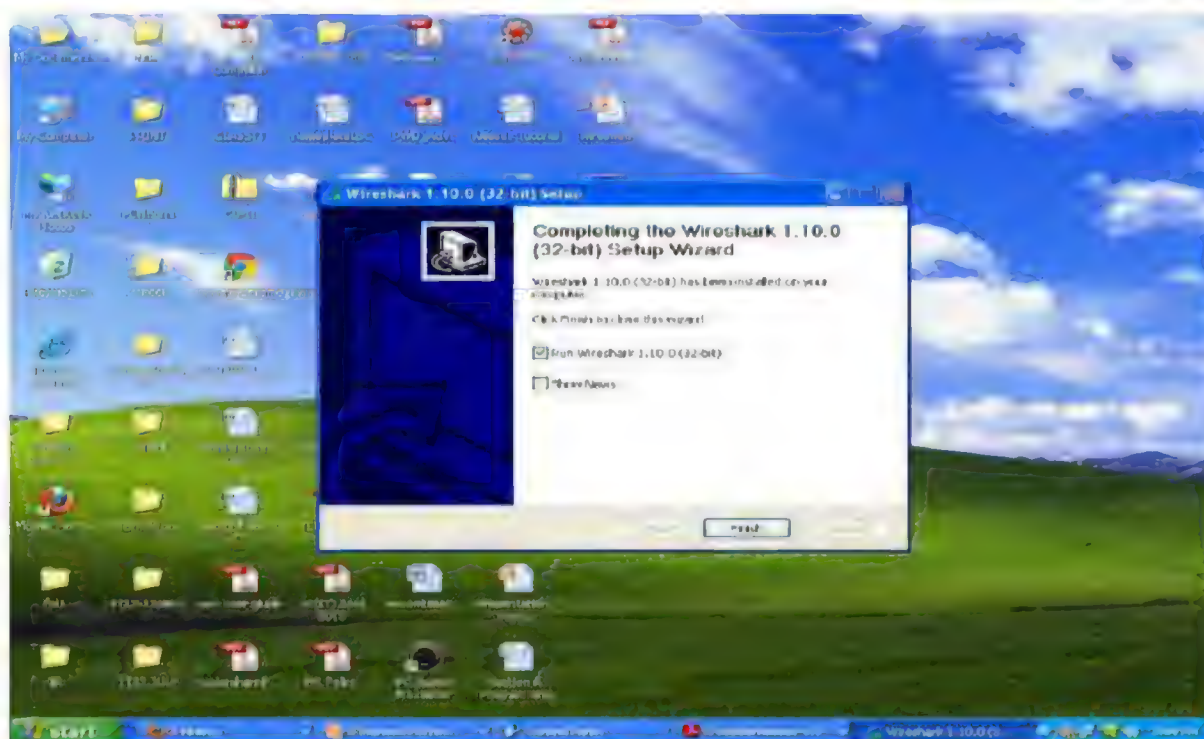


STEP : 9

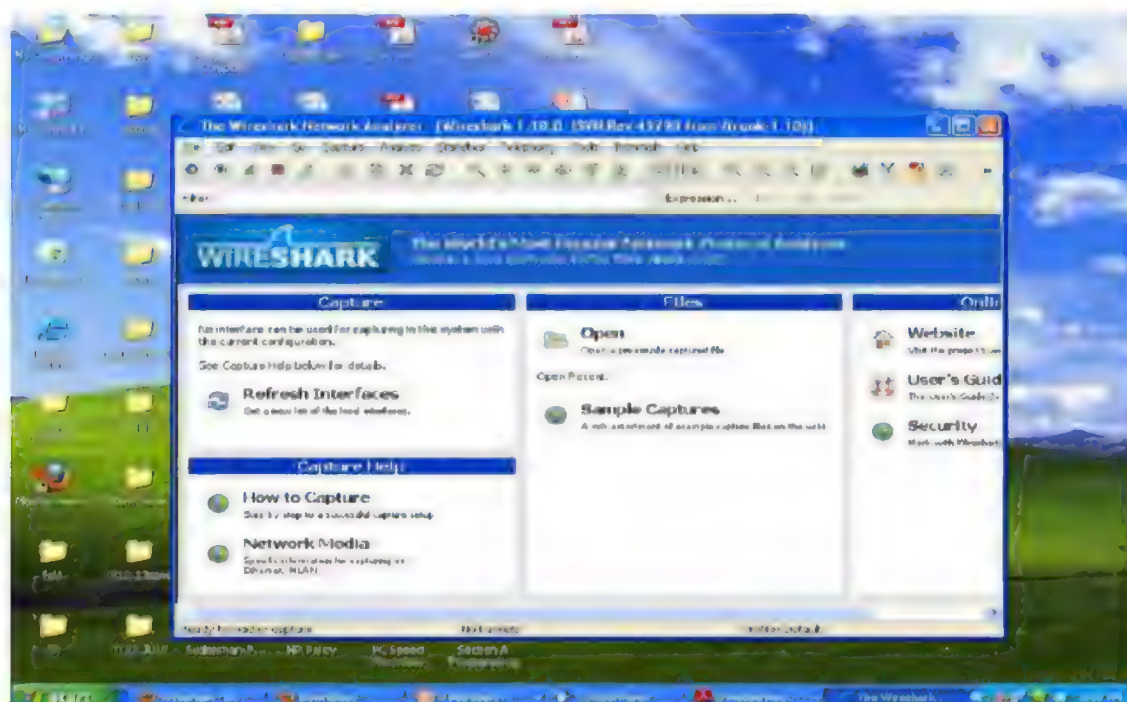




STEP :11



STEP : 12



Wireshark Graphical User Interface

When you run the Wireshark program, the Wireshark graphical user interface shown in Figure 2 will be displayed. Initially, no data will be displayed in the various windows.

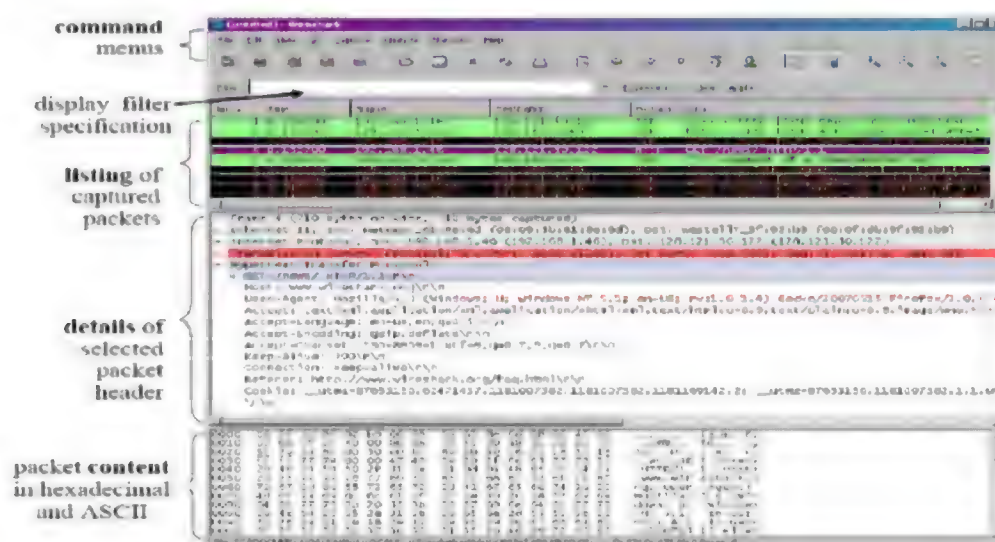
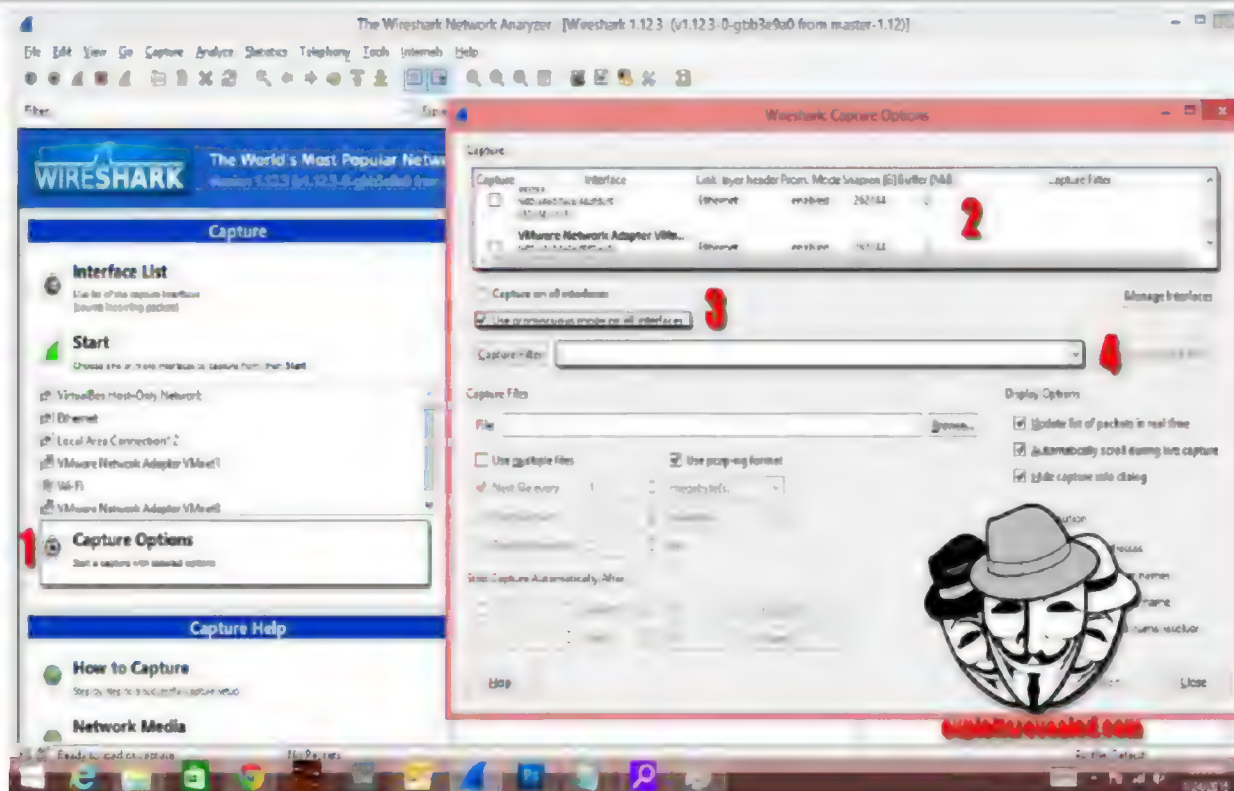
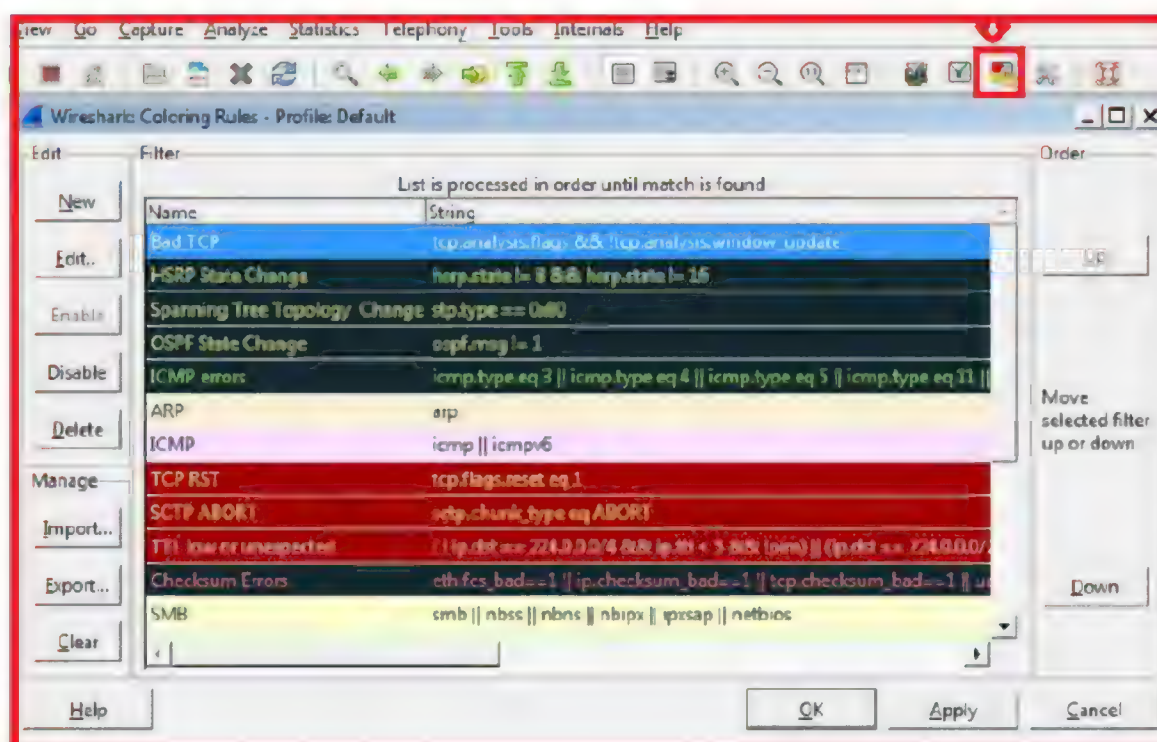
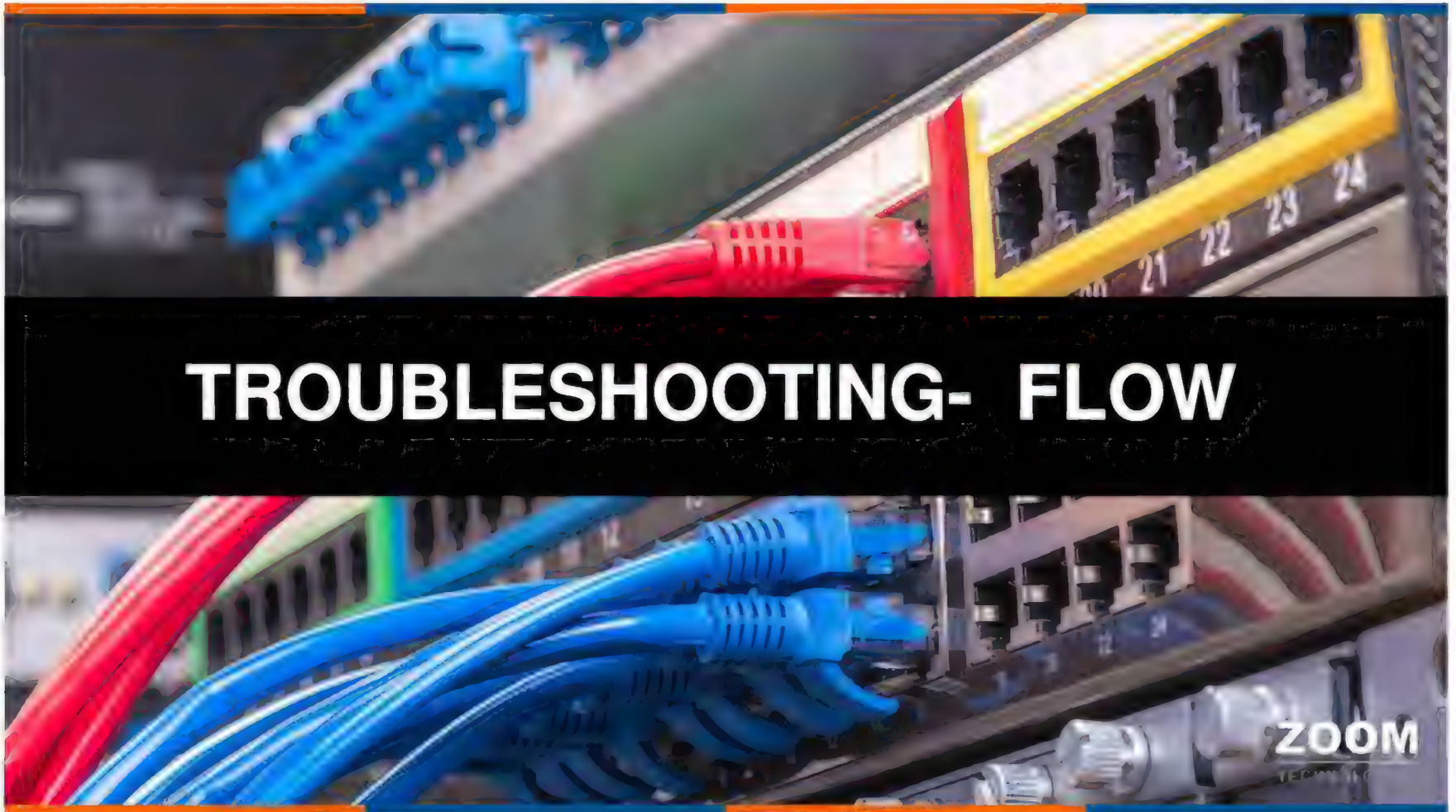


Figure 2: Wireshark Graphical User Interface



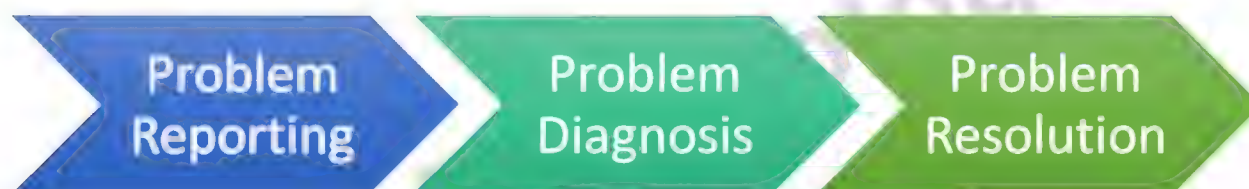
WIRESHARK COLOR CODED





Troubleshooting Flow

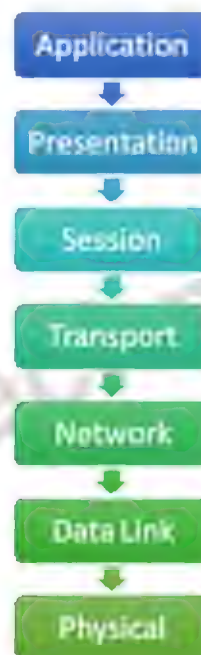
ZOOM
TECHNOLOGIES

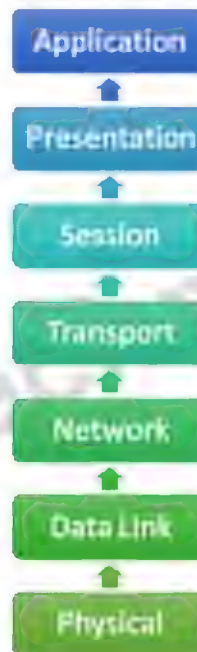


Popular Troubleshooting Methods

- Top-down method
- Bottom-up method
- Divide and Conquer method
- Following the Traffic path
- Comparing configurations
- Component swapping

Top-down method

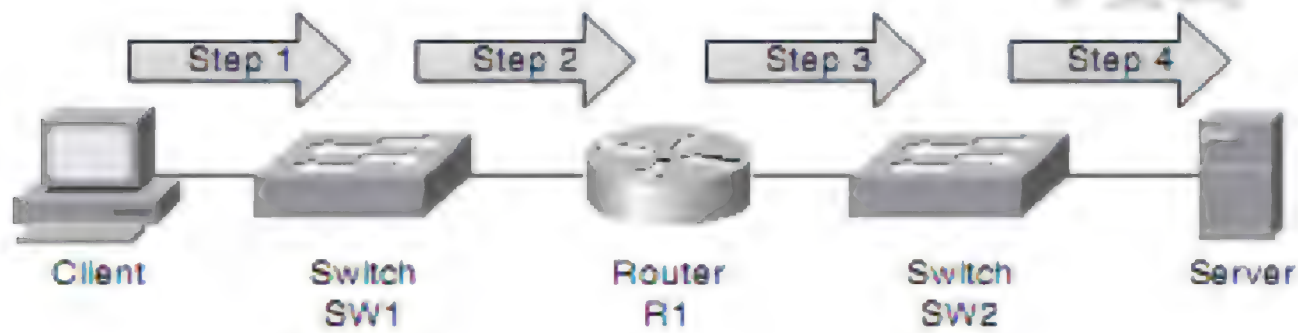




Ping 10.0.0.1

Follow the Traffic path method

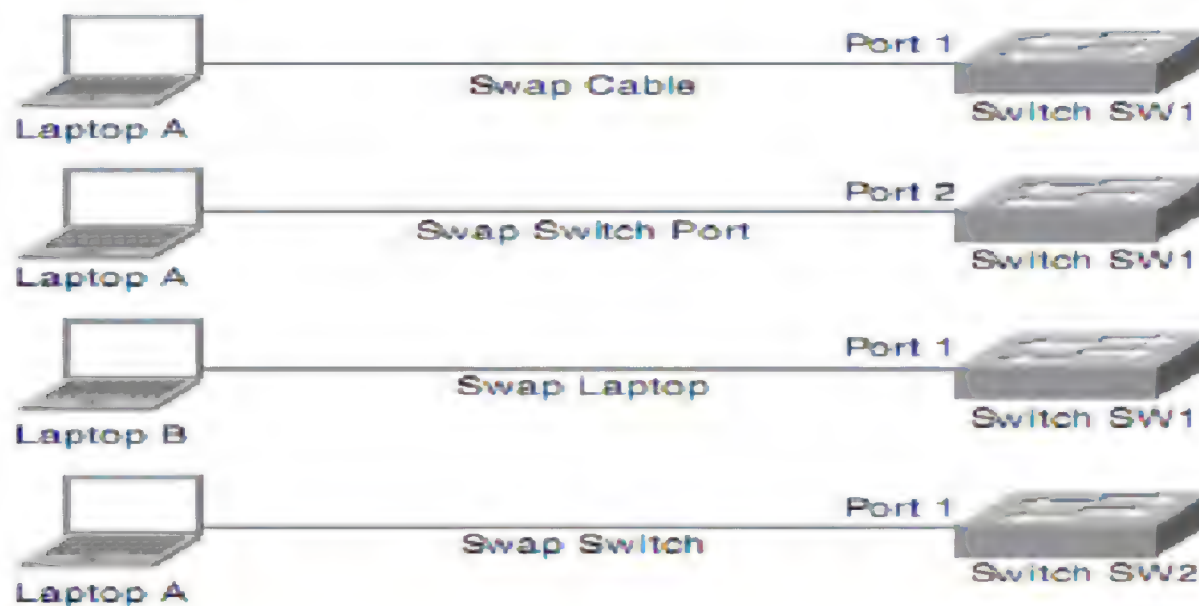
ZOOM
TECHNOLOGIES



CCIE
CCNP
CCNA

Component swapping

ZOOM
TECHNOLOGIES



CCIE
CCNP
CCNA

- **What is Network Maintenance?**
 - Doing whatever is required to keep the network functioning and meeting the business needs of an organization.
- It is a very important responsibility or duty of the Network Administrator
- It could also be a response to a reported problem
- Proactively performing regular scheduled maintenance tasks reduces problems



- CLI Tools
- GUI Tools
- Backup tools
- Logging Tools
- Network Time Protocol
- Network Documentation Tools



Examples of Network Maintenance



- Hardware and Software installation and configuration
- Monitoring and Tuning Network performance
- Network expansion planning
- Documentation of Network changes
- Compliance with legal regulations and corporate policies
- Securing the Network from Internal and External threats



Common Elements in Network Documentation



- Logical Topology Diagram
- Physical Topology Diagram
- Interconnections list
- Inventory of Network equipment
- IP Address Assignment
- Configuration Information
- Original Design Document



ROUTE TROUBLESHOOTING

ZOOM

EIGRP Troubleshooting

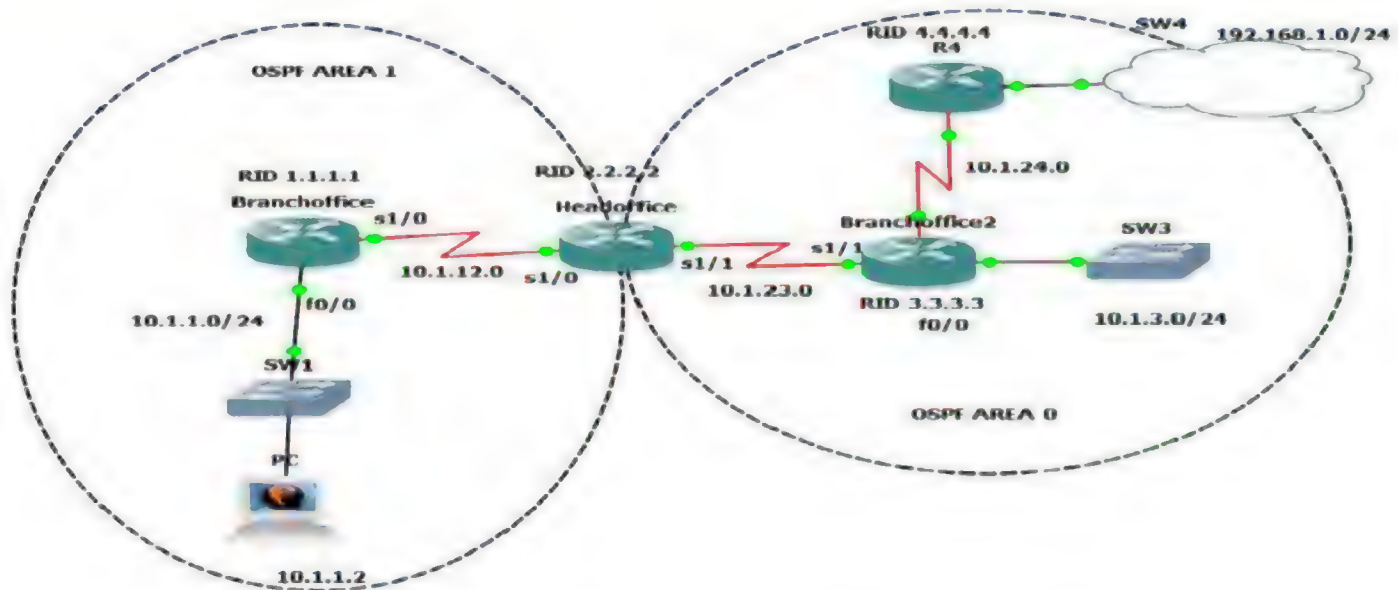
ZOOM
TECHNOLOGIES



User working in BranchOffice 1 is not able to communicate with user in Branch Office 2

- Interface is down
- Mismatched Autonomous Systems
- Incorrect Network Statement
- Mismatched K Values
- Passive Interface
- Different Subnet
- Authentication
- ACL
- Timers

Zoom Technologies



users in branchoffice 1 are not able to access the resources 192.168.1.0/24 network

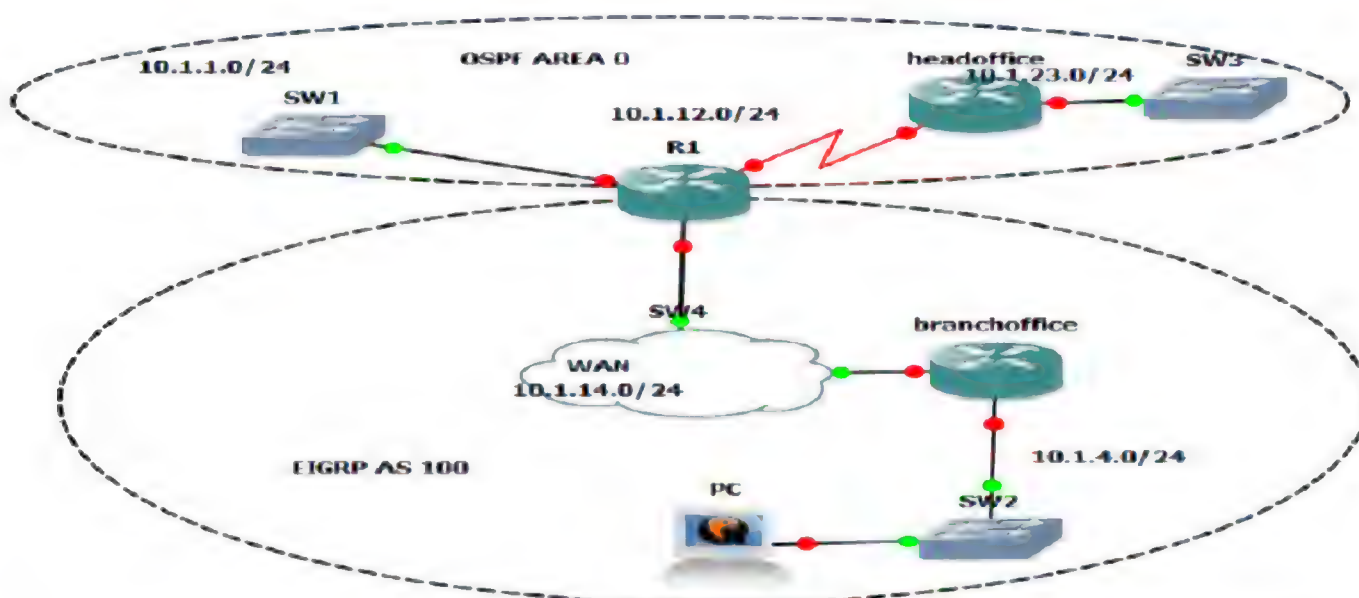
- Interface is down
- Interface not running the OSPF process.
- Mismatched timers.
- Mismatched area numbers
- Mismatched area type



- Different subnets
- Passive interface
- Mismatched authentication
- ACL
- MTU mismatch
- Duplicate Router ID
- Mismatched network types



- MTU mismatch :
- The maximum transmission unit of neighboring interfaces must match.
- Deliberately configure a different MTU on interfaces of two routers sharing a link
- Router(config)#int s1/0
- Router(config-if)#ip mtu 100
- Verify
- Router#Sh run interfaces s1/0
- After configuring verify by giving the neighbor command
- The state will be exstart



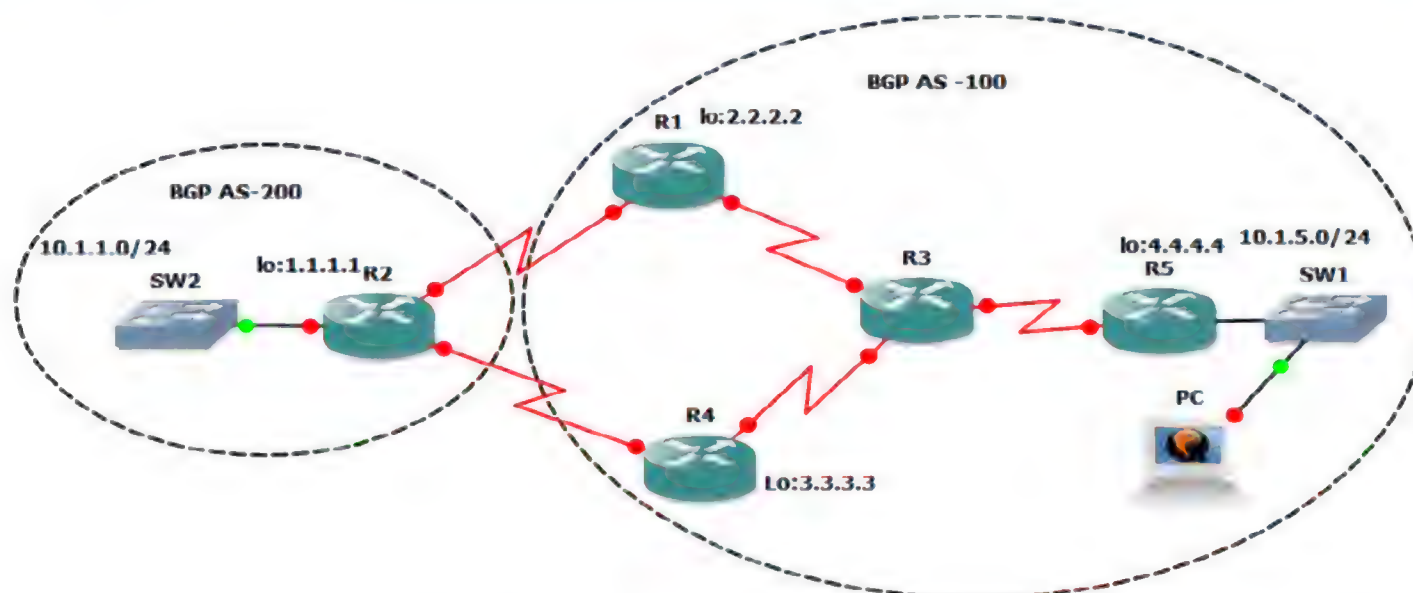
Users from branchoffice cannot communicate with any resources out side the branchoffice

Redistribution

- Distribute list
- Route-maps
- Metric
- AS number
- Process-id
- Hop count

Zoom Technologies

BGP Troubleshooting



you are the administrator for AS 100 ,the users from 10.1.1.0/24 network is not able to communicate to 10.1.5.0/24

BGP Troubleshooting



- Interface is down
- Layer 3 connectivity is broken
- Incorrect neighbor statement
- Incorrect network command
- BGP packets are sourced from wrong IP address
- Mismatched of Authentication
- Neighbor doesn't have a route

Zoom Technologies



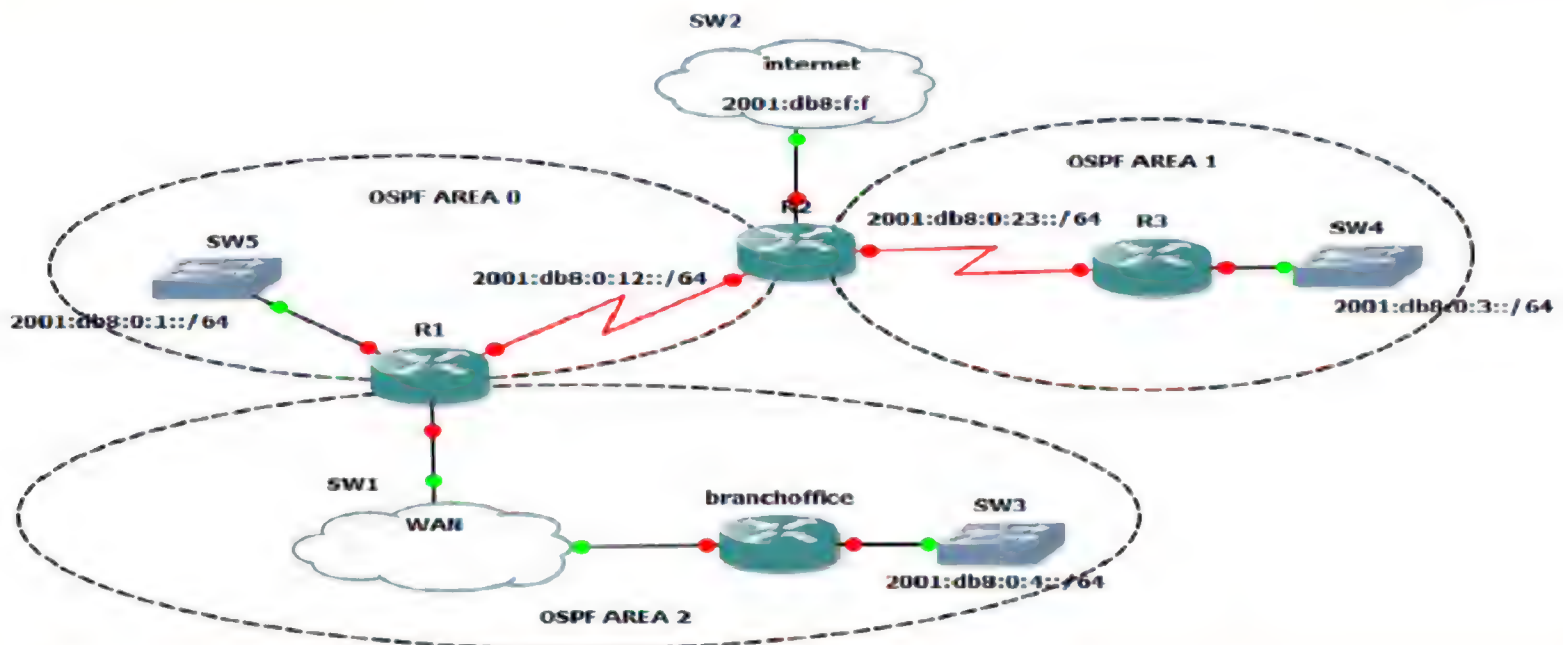
BGP Troubleshooting



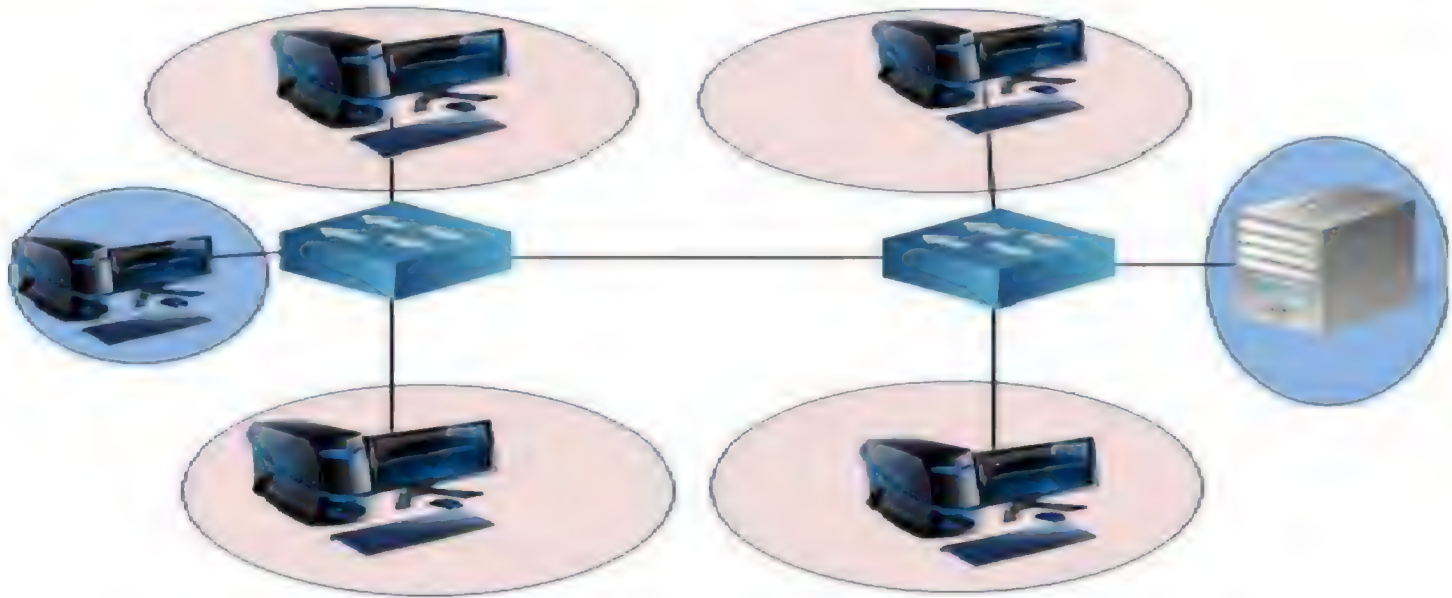
- Next hop router is not reachable
- BGP Split horizon
- BGP Synchronization
- Route Filtering

Zoom Technologies





SWITCH TROUBLESHOOTING



- Encapsulation Mismatch
- Incompatible Trunking modes
- Native Vlan Mismatch
- Allowed vlans
- VTP domain name mismatch

Zoom Technologies



- Domain name mismatch
- Version mismatch
- Mode mismatch
- Password mismatch

VTP domain name mismatch



- Sw_server(config) vtp domain zoom.com
- Sw_client(config) vtp domain zoom.com

Note : the domain name is only propagated in the beginning if it is null then it will join the first domain but when it is already part of a domain then it won't update the domain name. That has to be done manually also on the clients.

Zoom Technologies



VTP Troubleshooting



- Domain name mismatch
- Version mismatch
- Mode mismatch
- Password mismatch

Zoom Technologies



- Incorrect IP address
- Missing vlan
- Incorrect port Assignment

Zoom Technologies



STP Troubleshooting

ZOOM
TECHNOLOGIES

- No Trunking connectivity
- STP disabled
- Portfast
- BPDU Guard and BPDU filter
- Loop Guard

Zoom Technologies

CCIE
CCNP
CCNA

ETHERCHANNEL Troubleshooting

ZOOM
TECHNOLOGIES



Zoom Tev

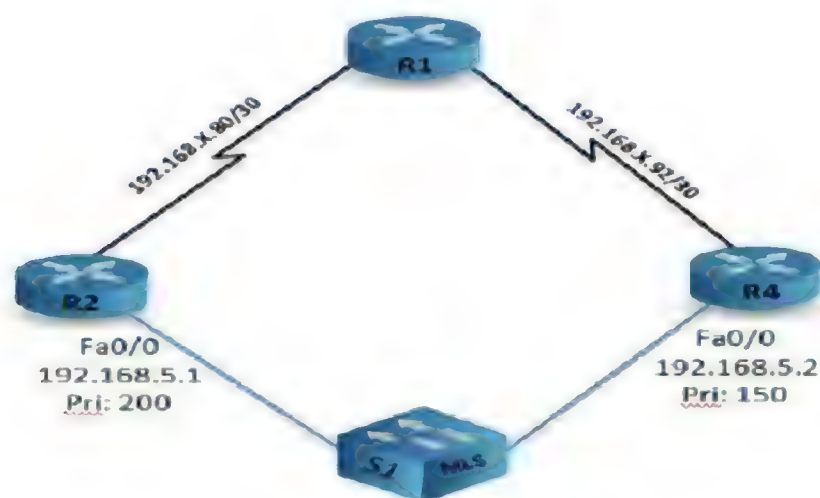
CCIE
CCNP
CCNA

- Mismatched Port configurations
- Mismatched Etherchannel Configuration
- Mismatch of Protocol





- Port security configured but not enabled
- A static MAC address was not configured correctly
- The maximum number of MAC addresses has been reached ,preventing access
- Legitimate users are being blocked because of violation
- Running configuration not saved to startup configuration



- Group number
- Same virtual IP address
- Priority
- Preemption
- Interface tracking

Zoom Technologies

MCSE-2012 Full Course

MICROSOFT CERTIFIED SOLUTIONS EXPERT

Practicals in real-time environment. Detailed curriculum with all 5 papers

Duration: 1 Month | 4 Hrs Per Day (starts on 15th & 30th of every month)

Batches: Morning: 8.30 to 10.30 • Afternoon: 2.00 to 4.00 • Evening: 7.30 to 9.30

CCNA (v 2.0) Full Course

CISCO CERTIFIED NETWORK ASSOCIATE

Cisco Routers with BSNL/TELCO MUX & Live Channelled E1

Duration: 1 Month | 4 Hrs Per Day (starts on 15th & 30th of every month)

Batches: Morning: 8.30 to 10.30 • Afternoon: 2.00 to 4.00 • Evening: 7.30 to 9.30

LINUX ADMINISTRATION

COMPLETE RHCE LINUX

Practicals on Live Web Administration + Integration of Windows with Linux/Unix (Samba Server)

Duration: 2 Weeks | 4 Hrs Per Day (starts on 15th & 30th of every month)

Batches: Morning: 8.00 • Afternoon: 1.30 • Evening: 7.00

PC HARDWARE & NETWORKING

WORKSHOP ON EMERGING TECHNOLOGIES

- Ethical Hacking, Cyber Security and Firewall
- Open Source: A glimpse into advance Linux
- VMware vSphere and MS Private Clouds
- Cisco WAN Technology & Collaboration

Free MCSE & CCNA Exam Practice Questions

EHCE | Ethical Hacking & Countermeasures Expert

Course is mapped to EHCE course from US-Council (www.us-council.com)

(Pre requisite is CCNA / MCSE / LINUX)

Duration: 2 Weeks | 4 Hrs Per Day (starts on 15th & 30th of every month)

Batches: Morning: 7.30 or Evening: 6.00

Fees: ₹ 9,500/-

+ 14% Service Tax

CCNP R&S

CISCO CERTIFIED NETWORK PROFESSIONAL

Duration: 1 Month | 4 Hrs Per Day (starts on 15th of every month)

Batches: Morning: 7.30 • Afternoon: 2.00 • Evening: 6.00

- Labs on latest routers with IOS version 15.X

Monitoring, Diagnostics & Troubleshooting Tools

- PRTG • Wireshark • SolarWinds, etc.

Exam Practice Challenge Labs

CCIE R&S

CISCO CERTIFIED INTERNETWORK EXPERT

Duration: 1 Month | 4 Hrs Per Day (starts on 15th of every month)

Batches: Morning: 7.30 • Evening: 6.00

- Individual Rack For Every Student
- Real time scenarios by 20+ years experienced CCIE certified industry expert who has worked on critical projects worldwide.

Written + Lab Exam Focus

FREE Full Scale 8 Hours Exam Lab Included

Unlimited Lab Access For 1 Year

Complete Package
for Only

Fees: ₹ 5,900/-

+ 14% Service Tax

**Duration: 3 Months
4 Hrs Per Day**

100%

**GUARANTEED
JOB**

ASSISTANCE

Fees: ₹ ~~10,000/-~~

Introductory Special Offer

Fees: ₹ 5,500/-

+ 14% Service Tax

Fees: ₹ ~~25,000/-~~

Introductory Special Offer

Fees: ₹ 9,999/-

+ 14% Service Tax

MICROSOFT EXCHANGE SERVER-2013

Duration: 2 Weeks | 4 Hrs Per Day (starts on 15th & 30th of every month)
Batches: (Contact the Counselors for the next available batch)

Fees: ₹ 2,500/-
+ 14% Service Tax

MICROSOFT PRIVATE CLOUD

Microsoft Certified Solutions Expert [MCSE] Private Cloud

Duration: 2 Weeks | 4 Hrs Per Day

Batches: (Contact the Counselors for the next available batch)

Fees: 2,500/-
+ 14% Service Tax

ADVANCED LINUX

Duration: 2 Weeks | 4 Hrs Per Day (starts on 15th & 30th of every month)
Batches: (Contact the Counselors for the next available batch)

Fees: ₹ 2,500/-
+ 14% Service Tax

CCNA SECURITY

(Pre requisite is CCNA R&S)

CISCO CERTIFIED NETWORK ASSOCIATE - SECURITY

Duration: 2 Weeks | 4 Hrs Per Day (starts on 15th of every month)

Batches: Morning: 7.30 or Evening: 6.00

Fees: ₹ 7,500/-
+ 14% Service Tax

CCNP SECURITY

(Pre requisite is CCNA Security at ZOOM)

CISCO CERTIFIED NETWORK PROFESSIONAL - SECURITY

Duration: 2 Weeks | 4 Hrs Per Day (starts on 30th of every month)

Batches: Morning: 7.30 or Evening: 6.00

Fees: ₹ 9,500/-
+ 14% Service Tax

CCIE SECURITY

(Pre requisite is CCNA & CCNP Security at ZOOM)

CISCO CERTIFIED INTERNETWORK - SECURITY

Duration: 1 Month | 4 Hrs Per Day

Batches: (Contact the Counselors for the next available batch)

Fees: ₹ 15,500/-
+ 14% Service Tax

VMware vSphere

(Pre requisite is MCSE)

Duration: 1 Month | 4 Hrs Per Day (starts on 15th of every month)

Batches: Morning: 7.30 and Evening: 7.30

Fees: ₹ 4,950/-
+ 14% Service Tax

VMware vCloud

(Pre requisite is VMware vSphere)

Duration: 1 Week | 4 Hrs Per Day (starts on 15th of every month)

Batches: Morning: 9.30 to 11.30

Fees: ₹ 2,500/-
+ 14% Service Tax

CHECKPOINT FIREWALL

Duration: 2 Weeks | 4 Hrs Per Day

Batches: (Contact the Counselors for the next available batch)

Fees: ₹ 5,500/-
+ 14% Service Tax

We also offer the following courses (Contact the Counselors for the next available batch)

- | | | | |
|------------------------------------|-------------|---------------------------|-------------|
| › CCNA Voice | @ ₹7,500/- | › CCNA Data Center | @ ₹7,500/- |
| › CCNP Voice | @ ₹9,500/- | › CCNP Data Center | @ ₹9,500/- |
| › CCIE Collaboration | @ ₹15,500/- | › CCIE Data Center | @ ₹15,500/- |
| › IPv6 Migration @ ₹5,500/- | | | |

FACULTY

- › All Senior Engineers of Zoom working on Live projects
- › Training Engineers of British Army, CISCO, CMC, GE, BSNL, Tata Teleservices and Several Corporates etc for 18 Years.

FREE Training

Zoom Technologies offers a number of free resources for the professional development of network engineers.

Register on our website to get access to the video recordings of live sessions on:

- **MCSE – Windows Server 2012**
 - **Cisco – CCNA**
 - **Cisco – CCNP**
 - **Cisco – CCIE**
 - **Exchange Server 2013**
 - **Linux**
 - **Advanced Linux**
 - **Ethical Hacking and Countermeasure Expert (www.us-council.com)**
- } All Tracks (R & S, Security and Voice)
- } All Flavors

Find us at: www.zoomgroup.com

Like us on Facebook and get access to free online webinars as well as special offers and discounts.
<https://www.facebook.com/ZoomTechnologies>

Online Training

Online Training at Zoom is a cost effective method of learning new networking skills from the convenience of your home or workplace.

Taking an online training course has many advantages for everyone (Freshers / Working Professionals). Zoom offers online training for the highly coveted CCNA, CCNP and CCIE courses as well as MCSE, Linux, VMware, Ethical Hacking and Firewalls, IPv6 with more courses planned for the near future. These are live instructor led courses, using Cisco WebEX. Check out our online course offerings at: http://zoomgroup.com/online_course

Job Opportunities

There is a high demand for network and security professionals at all times. Apart from job opportunities in India and the Middle East, network and security administrators are also sought-after in the US and Europe.

If you do not have the right skills, then get them now! Choose the experts in network and security training, an organization which has already trained over one hundred thousand engineers.

For the latest job openings in networking and security, register and upload your resume on: <http://zoomgroup.com/careers> or visit zoom to choose job offering from several multinational companies.





ABOUT US

Zoom Technologies India Pvt. Ltd. is a pioneering leader in network and security training, having trained over a hundred thousand engineers over the last two decades.

We offer a world class learning environment, with state-of-the-art labs which are fully equipped with high-end routers, firewalls, servers and switches. All our courses are hands-on so you'll get much needed practical experience.

The difference between us and the competition can be summed up in one simple sentence. Our instructors are real-time network professionals who also teach.

Zoom has designed, developed and provided network and security solutions as well as training to all the big names in the Indian industry, for the public sector as well as corporate leaders. Some of our clients are:

TATA
BSNL
VSNL
Indian Railways
National Police Academy
Air Force Academy
IPCL- Reliance Corporation
CMC
British Army

No other training institute can boast of a customer base like this. This is the reason for the resounding success of our networking courses. If you do not have the right skills, then get them now. Come, join the experts!

Training Centers in Hyderabad, India.

Banjara Hills

HDFC Bank Building, 2nd Floor,
Road # 12, Banjara Hills,
Hyderabad - 500 034
Telangana,
India.

Phone: +91 40 23394150
Email: banjara@zoomgroup.com

Ameerpet

203, 2nd Floor,
HUDA Maitrivanam, Ameerpet,
Hyderabad - 500 016
Telangana,
India.

Phone: +91 40 39185252
Email: ameerpet@zoomgroup.com

Secunderabad

Navketan Building,
5 Floor, # 501
Secunderabad - 500 003
Telangana,
India.

Phone: +91 40 27802461
Email: mktg@zoomgroup.com

Dilsukhnagar

1st Floor, # 16-11-477/B/1&B/2,
Shlivahana Nagar, Dilsukhnagar,
Hyderabad - 500 060
Telangana,
India.

Phone: +91-40-24140011
Email: dsnr@zoomgroup.com

website: www.zoomgroup.com

